A RECURSIVE TOWER OF FUNCTION FIELDS OVER $\mathbb{F}_2$

by

SEHER TUTDERE

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

Fall 2009

A RECURSIVE TOWER OF FUNCTION FIELDS OVER $\mathbb{F}_2$

APPROVED BY

Prof. Dr. Henning Stichtenoth (Thesis Supervisor) .....

Prof. Dr. Alev Topuzoğlu .....

Assist. Prof. Dr. Cem Güneri .....

Assoc. Prof. Dr. Wilfried Meidl .....

Assoc. Prof. Dr. Mehmet Keskinöz .....

DATE OF APPROVAL: January 21, 2009

A RECURSIVE TOWER OF FUNCTION FIELDS OVER $\mathbb{F}_2$

Seher Tutdere

Mathematics, Master Thesis, 2009

Thesis Supervisor: Prof. Dr. Henning Stichtenoth

Keywords: Finite fields, function fields, towers of function fields, rational places, genus.

Abstract

In 1995 Garcia and Stichtenoth gave explicit constructions of sequences of function fields over the finite field $\mathbb{F}_q$. Moreover, in the case that $q = p^k$ (for $k \geq 2$ and p is a prime) they have given some examples of towers having positive limit. The problem is how to construct towers of function fields over the prime fields $\mathbb{F}_p$ with positive limit. In this thesis we give an example of recursive towers $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields over the finite field $\mathbb{F}_2$. In this example all steps F_{i+1}/F_i are Artin-Schreier extensions. Although we cannot determine whether the limit of the tower $\mathcal{F}$ is positive or not, we give some asymptotics for the genus and the number of rational places in this tower.

$\mathbb{F}_2$ ÜZERİNDE ÖZYİNELİ BİR FONKSİYON CİSİMLERİ KULESİ

Seher Tutdere

Matematik, Yüksek Lisans Tezi, 2009

Tez Danışmanı: Prof. Dr. Henning Stichtenoth

Anahtar Kelimeler: Sonlu cisimler, fonksiyon cisimleri, fonksiyon cisimleri kuleleri, rasyonel yerler, cins

Özet

1995 yılında Garcia ve Stichtenoth $\mathbb{F}_q$ üzerinde bir fonksiyon cisimleri kulesinin bir polinom ile açık inşasını göstermişlerdir. Ayrıca, $q = p^k$ ($k \geq 2$ ve p bir asal sayı) olduğu durumlarda, limiti pozitif olan kule örnekleri vermişlerdir. Ancak, henüz F_p üzerinde limiti pozitif olan ve bir polinom tarafından ifade edilebilen herhangi bir kule tanımlanamamıştır. Bu tezde, $\mathbb{F}_2$ üzerinde $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ özyineli fonksiyon cisimleri kulelerine bir örnek verilmiştir. Bu örnekte, F_{i+1}/F_i genişlemeleri Artin-Schreier genişlemeleridir. Bu kulenin limiti ile ilgili bir sonuç elde edilememiştir. Ancak, bu kuledeki cins ve rasyonel yerler için bazı asimptotik sonuçlar verilmiştir.

Anneme

Acknowledgments

First I am very grateful to my advisor, Prof. Dr. Henning Stichtenoth, for his motivation, invaluable advice and encouragement throughout this thesis and his patience with even my trivial questions.

I am also very grateful to my family who have motivated and supported me throughout my whole life, especially to my brother for constant support during my studies.

I would like to thank Dr. Ayça Çeşmelioğlu for her help, especially whose computer knowledge I could not have done without. I also wish to thank Özgür and Nurdagül for being two excellent friends.

Furthermore, I would like to thank all my friends in Mathematics programs for all the useful discussions we made and enjoyable moments we shared.

Table of Contents

Introduction

Let F be an algebraic function field with the finite field $\mathbb{F}_q$ as its full constant field. Throughout this thesis, we shall simply refer to $F/\mathbb{F}_q$ as a function field. We denote by $N(F)$ its number of $\mathbb{F}_q$-rational places and $g(F)$ its genus. For a tower of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$ (see Definition 1.1), the limit $\lambda(\mathcal{F})$ of the tower $\mathcal{F}$ is defined as

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}.$$

Ihara introduced a quantity $A(q)$ as

$$A(q) := \limsup_{F} \frac{N(F)}{g(F)},$$

where F runs over all function fields over $\mathbb{F}_q$ with $g(F) > 0$. Furthermore, Drinfeld and Vladut proved, [1, p.244], that

$$A(q) \leq q^{1/2} - 1.$$

In the case that $q = p^{2k}$ (for $k \geq 1$ and p a prime) is a square, it was first shown by Ihara and Tsfasman, Vladut and Zink that the equality holds, by using the theory of modular curves. But then Garcia and Stichtenoth gave a more elementary proof by defining a tower over $\mathbb{F}_q$ whose limit attains this bound, see [1, p.265]. It is also clear that

$$0 \leq \lambda(\mathcal{F}) \leq A(q).$$

We say that a tower $\mathcal{F}$ is

$$\begin{aligned} \textit{asymptotically good,} \text{ if } \quad & \lambda(\mathcal{F}) > 0, \\ \textit{asymptotically bad,} \text{ if } \quad & \lambda(\mathcal{F}) = 0, \\ \textit{optimal,} \text{ if } \quad & \lambda(\mathcal{F}) = A(q). \end{aligned}$$

In general, the main aim is to construct "asymptotically good" towers $\mathcal{F} = (F_0, F_1, \ldots)$ over the finite field $\mathbb{F}_q$. That means; each function field $F_n/\mathbb{F}_q$ has many rational places compared to its genus. In the case that $q = p^e$ (p a prime) with $e > 1$, there are asymptotically good recursive towers $\mathcal{F}$ over the field $\mathbb{F}_{p^e}$ (see the references). The problem is how to find non-constant polynomials which define towers $\mathcal{F}$ with positive limit $\lambda(\mathcal{F}) > 0$ over the fields $\mathbb{F}_p$.

In this thesis, we investigate the tower of function fields $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ which is recursively defined by the polynomial

$$f(X, Y) = Y^2X + Y + X^2 + 1 \qquad (*)$$

over the field $\mathbb{F}_2$. It turns out that for the first members of this tower, the quotient $N(F_i)/g(F_i)$ is rather big, and so $\mathcal{F}$ is an interesting tower over $\mathbb{F}_2$. We try to find out the limit of this tower. However, although we study with a simple polynomial over $\mathbb{F}_2$, we cannot determine the asymptotic behaviour of the tower $\mathcal{F}$, i.e., we do not know whether this tower is an asymptotically good tower or not. We give some bounds for the number of rational places and the genus of F_n for all $n \geq 0$.

- In Chapter 1, we introduce some notation and recall briefly basic definitions and properties of towers. In addition, we recall *Artin-Schreier extensions* with some other basic facts and prove that the polynomial (*) defines a recursive tower over $\mathbb{F}_2$.

- In Chapter 2, we start by investigating the basic function field of the tower $\mathcal{F}$, which is given by the equation

$$y^2x + y + x^2 + 1 = 0 \quad \text{over} \quad \mathbb{F}_2.$$

- In Chapter 3, we investigate the behaviour of the genus and the number of rational places of F_0 to F_6.

- Chapter 4 is devoted to some observations on the asymptotic behaviour of the genus and the number of rational places in the tower $\mathcal{F}$ which is defined by the polynomial (*).

1

Preliminaries

Let us first fix some notation. We consider function fields F/K where K is the full constant field of F. In this thesis, K will be the finite field $K = \mathbb{F}_2$. We denote by $\mathbb{P}_F$ the set of places of F/K. For a rational function field $K(x)$ we will write $(x = a)$ for the place which is the zero of $x - a$ (where $a \in K$) and $(x = \infty)$ for the pole of x. For a place P of F/K, we will use the following notations:

- $v_P :=$ the discrete valuation of F/K associated to the place P,
- $\mathcal{O}_P :=$the valuation ring of the place P,
- $\bar{F} := F_P$ is the residue class field of P,
- $\bar{x} := x(P) \in \bar{F}$ is the residue class of $x \in \mathcal{O}_P$.

For a finite separable extension E of F and a place $Q \in \mathbb{P}_E$, we will write $Q|P$ if the place Q lies over the place $P \in \mathbb{P}_F$. In this case, we will denote by $e(Q|P)$ and $d(Q|P)$ the ramification index of $Q|P$ and the different exponent of $Q|P$, respectively.

Definition 1.1. A tower $\mathcal{F}$ of function fields over K is an infinite sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ of function fields F_n/K having the following properties:

(a) $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \ldots$.

(b) The field K is the full constant field of F_n, for $n = 0, 1, 2, \ldots$.

(c) For each $n \geq 0$, the extension F_{n+1}/F_n is finite and separable.

(d) $g(F_i) \geq 2$ for some $i \geq 0$.

Definition 1.2. Let $f(X, Y) \in \mathbb{F}_q[X, Y]$ be a non-constant polynomial, and let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a sequence of function fields. Suppose that there exist elements $x_n \in F_n$ (for $n = 0, 1, 2, \ldots$) such that

(i) for all $n \geq 0$ the elements x_n, x_{n+1} satisfy $f(x_n, x_{n+1}) = 0$,

(ii) x_0 is transcendental over $\mathbb{F}_q$ and $F_0 = \mathbb{F}_q(x_0)$, i.e., F_0 is a rational function field,

(iii) $F_n = \mathbb{F}_q(x_0, x_1, x_2, \ldots, x_n)$ for all $n \geq 0$,

(iv) $[F_1 : F_0] = \deg_Y f(X,Y)$ and $[F_1 : \mathbb{F}_q(x_1)] = \deg_X f(X,Y)$.

Then we say that the sequence $\mathcal{F}$ is *recursively* defined by the polynomial $f(X,Y)$ over the field $\mathbb{F}_q$.

Furthermore, a tower $\mathcal{F} = (F_0, F_1, \ldots)$ over $\mathbb{F}_q$ is called *tame* if for all $Q \in \mathbb{P}_{F_n}$ and $P \in \mathbb{P}_{F_0}$ with $Q|P$, we have that the ramification index $e(Q|P)$ is relatively prime to the characteristic of $\mathbb{F}_q$ for all $n \geq 1$; otherwise $\mathcal{F}/\mathbb{F}_q$ is called a *wild* tower.
We consider a recursive tower as a pyramid, which is the most appropriate way of working with recursive towers. As an example, we illustrate this way with the following picture that reaches the 5^{th} step of the tower (where $G_i := \mathbb{F}_2(x_1, \ldots, x_{i+1})$).

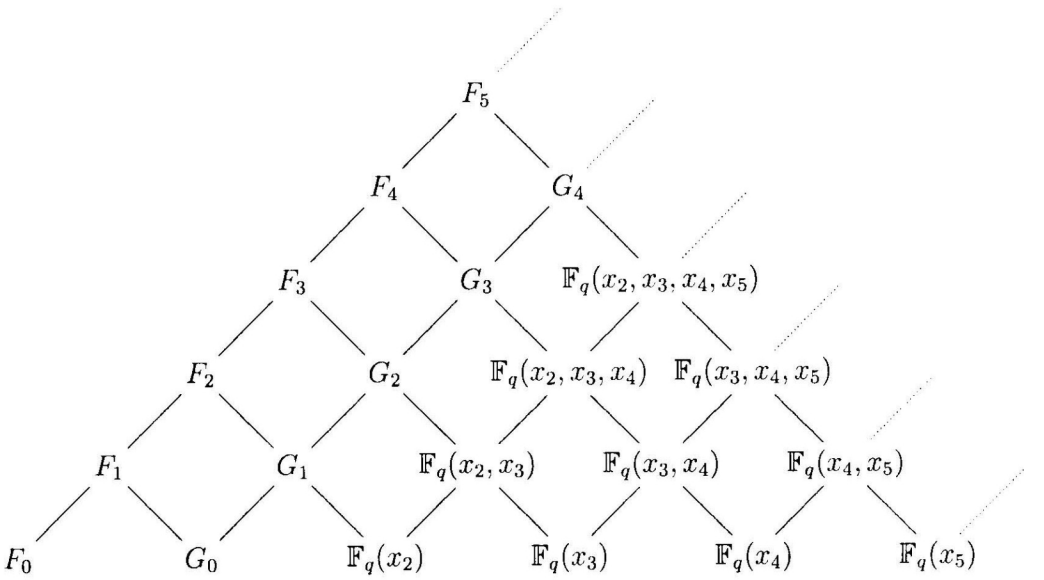


Figure 1.1: F_5

As seen in the above picture, all fields $\mathbb{F}_q(x_j, \ldots, x_m)$ with $0 \leq j \leq m \leq 5$ are shown in our pyramid. Further, all fields on the same horizontal line are isomorphic, for instance, $F_2 \cong G_2 \cong \mathbb{F}_q(x_2, x_3, x_4) \cong \mathbb{F}_q(x_3, x_4, x_5)$. Moreover, knowing the ramification indices and the different exponents in the base of the pyramid we can climb up by using the following useful methods:

Theorem 1.3 (Abhyankar's Lemma). *Let F'/F be a finite separable extension of function fields. Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields*

$F \subseteq F_1, F_2 \subseteq F'$. *Let* $P' \in \mathbb{P}_{F'}$ *be an extension of* $P \in \mathbb{P}_F$, *and set* $P_i := P' \cap F_i$ *for* $i = 1, 2$. *Assume that at least one of the extensions* $P_1|P$ *or* $P_2|P$ *is tame. Then*

$$e(P'|P) = lcm\left\{e(P_1|P),\ e(P_2|P)\right\},$$

where lcm stands for least common multiple.

Proof. For the proof see [1, p.137]. □

Theorem 1.4 (Transitivity of the Different Exponent). *Let* $F \subseteq F' \subseteq F''$ *be a tower of finite separable extensions. If* P, P', P'' *are places of* F, F', F'', *respectively, with* $P''|P'|P$, *then the following holds:*

$$d(P''|P) = e(P''|P')d(P'|P) + d(P''|P').$$

Proof. See [1, p.98]. □

To compute the genus of F_i for each $i \geq 0$, we need the following theorem:

Theorem 1.5 (Hurwitz Genus Formula). *Let* F/K *be an algebraic function field of genus* g *and* F'/F *be a finite separable extension. Let* K' *denote the constant field of* F' *and* g' *the genus of* F'/K'. *Then we have*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg Diff(F'/F)$$

where $\deg Diff(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot \deg P'.$

Proof. See [1, p.99]. □

Theorem 1.6 (Artin-Schreier Extensions). *Let* F/K *be an algebraic function field of characteristic* $p > 0$. *Suppose that* $u \in F$ *is an element such that there exists a place* $Q \in \mathbb{P}_F$ *with*

$$v_Q(u) < 0 \quad and \quad v_Q(u) \not\equiv 0 \bmod p.$$

Let

$$F' = F(y) \quad with \quad y^p - y = u.$$

Such an extension F'/F *is called an Artin-Schreier extension of* F. *For* $P \in \mathbb{P}_F$ *we define the integer* m_P *by*

$$m_P := \begin{cases} m & \text{if there is an element } z \in F \text{ satisfying} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ and } m \not\equiv 0 \bmod p, \\ -1 & \text{if } v_P(u - (z^p - z)) \geq 0 \text{ for some } z \in F. \end{cases}$$

Then we have

(a) F'/F *is a cyclic Galois extension of degree* p,

(b) P *is unramified in* F'/F *iff* $m_P = -1$,

(c) P *is totally ramified in* F'/F *iff* $m_P > 0$. *If we denote by* P' *the unique place of* F' *lying over* P, *then the different exponent* $d(P'|P)$ *is given by*

$$d(P'|P) = (p-1)(m_P + 1).$$

Proof. See [1, p.127]. □

Remark 1.7. With the same notations as in the above theorem, if $v_P(u) = -m < 0$ and $m \not\equiv 0 \ mod\ p$, then P is totally ramified in F'/F and $v_{P'}(y) = -m$.

Proof. As P' lies over P, we have

$$v_{P'}(y^p - y) = e(P'|P)v_P(u) = -m \cdot e(P'|P) < 0, \text{ and so } p \cdot v_{P'}(y) = -m \cdot e(P'|P).$$

Hence, $v_{P'}(y) = -m$ and $e(P'|P) = p$ since p and m are relatively prime. □

Example: Let $q = 2$. We claim that the sequence $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ which is recursively defined over $\mathbb{F}_2$ by the polynomial

$$f(X, Y) = Y^2X + Y + X^2 + 1$$

is a tower over $\mathbb{F}_2$.

Thus, we need to prove the statements (a), (b), (c), (d) in the definition 1.1. To prove these, we will use the following useful lemma whose proof is trivial and can be omitted.

Lemma 1.8. *Consider a sequence of fields* $F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots$, *where* F_0 *is a function field with the constant field* $\mathbb{F}_q$ *and* $[F_{n+1} : F_n] < \infty$ *for all* $n \geq 0$. *Suppose that for all* n, *there exist places* $P_n \in \mathbb{P}_{F_n}$ *and* $Q_n \in \mathbb{P}_{F_{n+1}}$ *with* $Q_n|P_n$ *and ramification index* $e(Q_n|P_n) > 1$. *Then it follows that* $F_n \subsetneq F_{n+1}$.

If we assume furthermore that $e(Q_n|P_n) = [F_{n+1} : F_n]$ *for all* n, *then* $\mathbb{F}_q$ *is the constant field of* F_n *for all* $n \geq 0$.

Now we return to our example given above. Firstly, notice that $F_{n+1} = F_n(x_{n+1})$ and $x_{n+1}^2 x_n + x_{n+1} = x_n^2 + 1$, and so $[F_{n+1} : F_n] \leq 2$. For $n = 0$, we have

$$x_1^2 x_0 + x_1 = x_0^2 + 1.$$

Multiplying this equation by x_0, we obtain $x_1^2 x_0^2 + x_1 x_0 = x_0^3 + x_0$. Let $z_1 := x_1 x_0$. Then we get $z_1^2 + z_1 = x_0^3 + x_0$. Notice that $F_1 = \mathbb{F}_2(x_0, x_1) = \mathbb{F}_2(x_0, z_1)$. Let $P_\infty := (x_0 = \infty)$ be the pole of x_0 in $F_0 = \mathbb{F}_2(x_0)$. Then $v_{P_\infty}(x_0^3 + x_0) = -3$. Since $3 \not\equiv 0 \ mod\ 2$, we have an Artin Schreier extension of degree 2 by Theorem 1.6. That means, the

polynomial $x_0T^2 + T + x_0^2 + 1$ is irreducible and separable in $\mathbb{F}_2(x_0)[T]$. Notice that $T^2 + T + x_0^3 + x_0$ is the minimal polynomial of z_1 over F_0. Now since $m_{P_\infty} = 3 > 0$, P_∞ is totally ramified in F_1/F_0 and by Remark 1.7 we have $v_{P_1}(z_1) = -3$, where P_1 lies over P_∞ in F_1. Therefore, from the equation

$$\begin{aligned} v_{P_1}(z_1) &= v_{P_1}(x_1x_0) = v_{P_1}(x_1) + v_{P_1}(x_0) \\ &= v_{P_1}(x_1) + e(P_1|P_\infty) \cdot v_{P_\infty}(x_0) = v_{P_1}(x_1) + 2 \cdot (-1), \end{aligned}$$

we get $v_{P_1}(x_1) = -1$. That means; P_1 is a pole of x_1 in F_1. Next, let P_2 be a place in F_2 lying over P_1. Similarly, we see from the equation $z_2^2 + z_2 = x_1^3 + x_1$, where $z_2 := x_2x_1$, that P_1 is ramified in F_2 and P_2 is a pole of x_2 in F_2. Now if we proceed inductively, we get the places $P_{n+1} \in \mathbb{P}_{F_{n+1}}$ and $P_n \in \mathbb{P}_{F_n}$ with P_{n+1} lies over P_n and $e(P_{n+1}|P_n) = 2$, for all $n \geq 0$. Hence, we have proved (a), (b), (c) by Lemma 1.8. Now it remains to prove (d).

Set $g_i := g(F_i)$ for all $i \geq 0$. Since $\mathbb{F}_2(x_0)/\mathbb{F}_2$ is a rational function field, $g_0 = 0$. Next, from the equation $z_1^2 + z_1 = x_0^3 + x_0$ we see that only the unique pole of x_0, P_∞ is ramified in F_1 by Theorem 1.6. Thus, by the same theorem, we get

$$d(P_1|P_\infty) = (p-1)(m_{P_\infty} + 1) = (2-1) \cdot (3+1) = 4. \tag{1.1}$$

Note that since all other places in F_0 are unramified in F_1, they do not contribute to the genus of F_1. Thus, by the Hurwitz-Genus Formula,

$$2g_1 - 2 = [F_1 : F_0](2 \cdot 0 - 2) + \deg Diff(F_1/F_0) = -4 + 4 = 0, \tag{1.2}$$

and so $g_1 = 1$. We know that in the extension F_2/F_1, there is at least one ramified place, namely P_2, and so $\deg Diff(F_2/F_1) \geq 1$. Again, by the Hurwitz Genus Formula, we get $g_2 \geq 2$. This proves (d). Therefore, the polynomial $f(X,Y) = Y^2X + Y + X^2 + 1$ defines a recursive tower $\mathcal{F} = (F_0, F_1, F_2, ...)$ over $\mathbb{F}_2$. Our main objective is to investigate this tower. We begin our study by introducing the notion of the *basic function field.*

2

The Basic Function Field

Definition 2.1. Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a tower of function fields which is recursively defined over $\mathbb{F}_q$ by a non-constant polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$. We define *the basic function field* of the tower $\mathcal{F}$ by

$$F := \mathbb{F}_q(x, y) \text{ with the relation } f(x, y) = 0.$$

It is clear that all subfields of F_n of the form $\mathbb{F}_q(x_i, x_{i+1})$ with $i \geq 0$ are $\mathbb{F}_q$-isomorphic to the basic function field $F = \mathbb{F}_q(x, y)$ under the map $x_i \mapsto x$ and $x_{i+1} \mapsto y$.

Now we are ready to treat the basic function field F of the tower $\mathcal{F}$ over $\mathbb{F}_2$ (see the example on p.4), which is given by the equation

$$y^2x + y + x^2 + 1 = 0 \quad \text{over} \quad \mathbb{F}_2, \tag{2.1}$$

i.e., $y^2x + y = x^2 + 1$.

Lemma 2.2. *The extension $F/\mathbb{F}_2(y)$ given by the above equation is an Artin-Schreier extension of degree* 2.

Proof. Let $t := \frac{x+y+1}{y^2}$. Observe that $\mathbb{F}_2(x, y) = \mathbb{F}_2(t, y)$. Then by using the equation (2.1), we get

$$\begin{aligned} t^2 + t &= \frac{x^2 + y^2 + 1}{y^4} + \frac{x + y + 1}{y^2} \\ &= \frac{y^2x + y + y^2 + xy^2 + y^3 + y^2}{y^4} \\ &= \frac{y + y^3}{y^4} = \frac{y^2 + 1}{y^3}. \end{aligned}$$

Notice that $v_{Q_0}(\frac{y^2+1}{y^3}) = -3 < 0$ and $3 \not\equiv 0 \ mod\ 2$ where $Q_0 = (y = 0)$ is the unique zero of y in $\mathbb{F}_2(y)$. Hence, by Theorem 1.6, Q_0 is ramified in $F/\mathbb{F}_2(y)$. Thus, the lemma follows. □

Note that by the same theorem, if P is the place of F lying above Q_0, then we have

$$d(P|Q_0) = (m_{Q_0} + 1)(p - 1) = (3 + 1)(2 - 1) = 4. \tag{2.2}$$

Our next aim is to find out the rational places of $F/\mathbb{F}_2$. To do this, let Q be a rational place of F. Since F and $\mathbb{F}_2(x)$ have the same constant field $\mathbb{F}_2$, if P is any place of $\mathbb{F}_2(x)$ lying below Q, then P also must be a rational place. Therefore, it is enough to find the rational extensions of the rational places of $\mathbb{F}_2(x)$. As $\mathbb{F}_2(x)/\mathbb{F}_2$ is a rational function field, the rational places of $\mathbb{F}_2(x)$ are as follows;

- the pole and the zero of x, denoted by $P_\infty = (x = \infty)$ and $(x = 0)$, respectively,
- the zero of $x + 1$, denoted by $(x = 1)$.

We know that $F = \mathbb{F}_2(x, y) = \mathbb{F}_2(x, z)$ (see p.4) where

$$z^2 + z = x^3 + x \quad \text{with} \quad z = xy.$$

From this equation, by Theorem 1.6, we can easily infer that the only ramified place of $\mathbb{F}_2(x)$ in F is the place $(x = \infty)$. Hence, P_∞ has only one extension, which is clearly rational. To find the extensions of $(x = 0)$ and $(x = 1)$, we will firstly introduce the following method.

Theorem 2.3 (Kummer). *Let F/K be a function field, and F'/F be a finite separable extension field. Let P be a place of F. Suppose that $F' = F(z)$, where z is integral over $\mathcal{O}_P$ with the minimal polynomial $\varphi(T)$. Assume that*

$$\bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)$$

is the decomposition of $\bar{\varphi}(T)$ into irreducible factors over $\bar{F}$ (i.e., the polynomials $\gamma_1, \ldots, \gamma_r$ are irreducible, monic and pairwise distinct in $\bar{F}[T]$). Choose monic polynomials $\varphi_i(T) \in \mathcal{O}_P[T]$ with

$$\bar{\varphi}_i(T) = \gamma_i(T) \quad \text{and} \quad \deg \varphi_i(T) = \deg \gamma_i(T).$$

Then there esists, for $1 \leq i \leq r$, exactly one place $P_i \in \mathbb{P}_{F'}$ with $P_i|P$ and $\varphi_i(z) \in P_i$. Further, the places $P_1, \ldots, P_r$ are all the places of F' lying over P, and we have

$$e(P_i|P) = 1 \quad \text{and} \quad f(P_i|P) = \deg \gamma_i(T).$$

Proof. See [1, p.68]. □

Lemma 2.4. *Let $F/\mathbb{F}_2$ be a function field, and $F' = F(z)$ be an Artin-Schreier extension field. Consider the minimal polynomial of z over F which is given as $\varphi(T) = T^2 + T + u$ where $u \in F$. Then for each rational place $P \in \mathbb{P}_F$ for which $v_P(u) > 0$, there are two rational extensions Q_1,$Q_2 \in \mathbb{P}_{F'}$ of P such that*

$$e(Q_i|P) = f(Q_i|P) = 1 \quad \text{for} \quad i = 1, 2$$

Moreover, $z \in Q_1$ i.e., $z(Q_1) = 0$ and $z + 1 \in Q_2$ i.e., $z(Q_2) = 1$.

Proof. Clearly, $v_P(u) > 0$ implies that $\varphi(T) \in \mathcal{O}_P[T]$. Then the decomposition of $\bar{\varphi}(T)$ into irreducible factors over $\bar{F}$ is

$$\bar{\varphi}(T) = T(T+1).$$

Hence, by the above Theorem 2.3, the result follows. □

Now we return to studying the rational places of $F = \mathbb{F}_2(x,y) = \mathbb{F}_2(x,z)$. We know that P_∞ has only one rational extension in F. Since $v(x^3+x) > 0$ at the places $(x=0)$ and $(x=1)$, by applying the above lemma, we conclude that each of these places has two rational extensions in F. Hence, there are totally 5 rational places of F, i.e., $N(F) = 5$. Note that since by definition F is isomorhic to F_1, the genus $g(F) = g(F_1) = 1$.

Let P, Q_1, Q_2, R_1, R_2 be all rational places of F such that $P|(x=\infty)$, $Q_i|(x=1)$ and $R_i|(x=0)$ for $i = 1,2$. Next, we want to find the restrictions of these places to $\mathbb{F}_2(y)$. Firstly, note that since F and $\mathbb{F}_2(y)$ have the same constant field $\mathbb{F}_2$, the restrictions of the rational places of F must be rational in $\mathbb{F}_2(y)$. Clearly, all rational places of $\mathbb{F}_2(y)$ are $(y=\infty)$, $(y=1)$, and $(y=0)$. We know that $F = \mathbb{F}_2(x,y) = \mathbb{F}_2(t,y)$, where

$$t^2 + t = \frac{y^2+1}{y^3},$$

and $F/\mathbb{F}_2(y)$ is an Artin-Schreier extension by Lemma 2.2. Moreover, we know that the only ramified place of $\mathbb{F}_2(y)$ in F is the zero of y, i.e., $(y=0)$. Since $v(\frac{y^2+1}{y^3}) > 0$ at the other places $(y=1)$ and $(y=\infty)$, by Theorem 1.6, they are unramified in F. Also, each of these places has two distinct rational extensions in F by Lemma 2.4. Now consider the place P lying over $(x=\infty)$. Since $(x=\infty)$ is ramified in F and we have $v_P(y) = -1$ by Remark 1.7, the restriction of P to $\mathbb{F}_2(y)$ is the pole of y. Next, consider the places Q_1 and Q_2 lying over $(x=1)$. Since $v_{Q_i}(x^3+x) > 0$ for $i = 1,2$, by Lemma 2.4, $z(Q_1) = 0$ and $z(Q_2) = 1$. Since $z(Q_i) = x(Q_i) \cdot y(Q_i)$ and $x(Q_i) = 1$ (for $i = 1,2$), it follows that $y(Q_1) = 0$ and $y(Q_2) = 1$. That means; $Q_1|(y=0)$ and $Q_2|(y=1)$. Now it remains to find the restrictions of R_i for $i = 1,2$. Since the only remaining rational places of $\mathbb{F}_2(y)$ are $(y=1)$ and $(y=\infty)$. Observe that each of these places has two extensions in F, $R_1|(y=1)$ and $R_2|(y=\infty)$. Furthermore, in the case that we have a ramified place we know the different exponents by the equations (1.1) and (2.2). We can summarize by the following pictures:

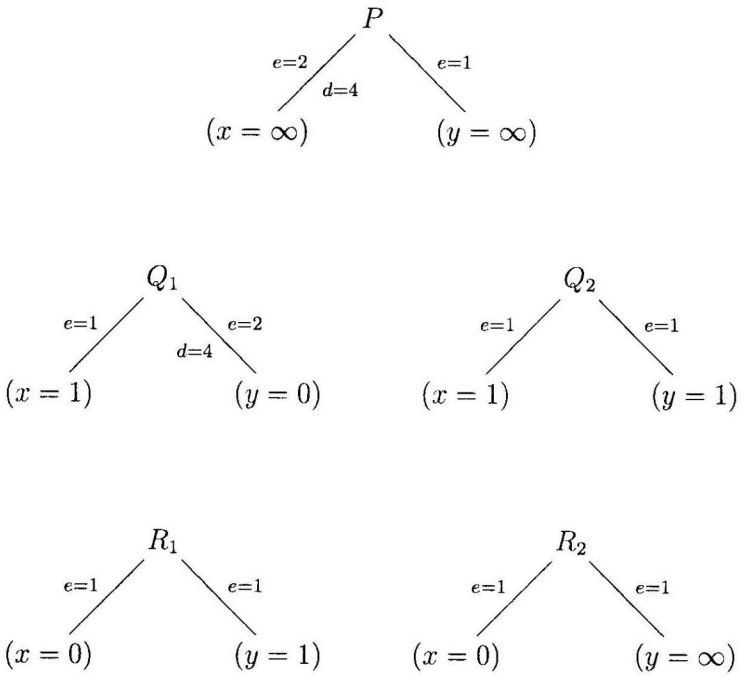


Figure 2.1: Rational places of F

Lemma 2.5. *Let $F = \mathbb{F}_2(x, y)/\mathbb{F}_2$ be the basic function field of the tower $\mathcal{F}$. Consider a place $P \in \mathbb{P}_F$ with $\deg P > 1$. Then P is unramified over both of the fields $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$. Further, the restriction of P to each of these fields is non-rational.*

Proof. Let $P \in \mathbb{P}_F$ with $\deg P > 1$. Then by Theorem 1.6, P is unramified over both of the fields $\mathbb{F}_2(x)$ and $\mathbb{F}_2(y)$. Since all rational places of both of these fields have rational extensions in F, the restriction of P to these fields must be non-rational. □

Here we remark that since the basic function field F has the genus $g(F) = 1$ and $N(F) = 5$, it is an example where Serre Bound, which is $N \leq q + 1 + [2q^{\frac{1}{2}}]$, is attained. Furthermore, one can prove that F is the only function field over $\mathbb{F}_2$ with this property (see [1], p.222).

3

A Wild Tower of Function Fields over $\mathbb{F}_2$

In the first chapter, we found out that the sequence of function fields $\mathcal{F} = (F_0, F_1, \ldots)$ which is recursively defined by the polynomial

$$f(X, Y) = Y^2X + Y + X^2 + 1 \tag{3.1}$$

is a tower over $\mathbb{F}_2$. That means;

$$F_0 = \mathbb{F}_2(x_0), \text{ and } F_{i+1} = F_i(x_{i+1}) \text{ for all } i \geq 0, \text{ where } \quad x_{i+1}^2 x_i + x_{i+1} = x_i^2 + 1.$$

Moreover, $F = \mathbb{F}_2(x, y)$ is the basic function field of the tower $\mathcal{F}$. Note that $\mathcal{F}$ is clearly a wild tower as there is a wildly ramified place, the pole of x, in F (i.e., characteristic of $\mathbb{F}_2$ divides the ramification index). Our main aim is to investigate this tower. That is, we want to find out the genus and the number of rational places of F_i, which are denoted by $g(F_i)$ and $N(F_i)$ for all $i \geq 0$, respectively.

Since F_0 is a rational function field, $g(F_0) = 0$. Also we know that there are three rational places of F_0, which are $(x_0 = 0)$, $(x_0 = 1)$, $(x_0 = \infty)$, i.e., $N(F_0) = 3$. In the previous chapter, we have already seen that $g(F_1) = g(F) = 1$ and $N(F_1) = N(F) = 5$. Now we move on to the next step, F_2. Our aim is to find the rational places and the genus of F_2, where $F_2 = F_1(x_2) = \mathbb{F}_2(x_0, x_1, x_2)$ with the equation

$$x_2^2 x_1 + x_2 = x_1^2 + 1,$$

which can be rewritten as

$$z_2^2 + z_2 = x_1^3 + x_1 \quad \text{where} \quad z_2 = x_2 x_1. \tag{3.2}$$

Let $G_0 := \mathbb{F}_2(x_1)$ and $G_1 := \mathbb{F}_2(x_1, x_2)$. Our pyramid reaches the *2nd* step as shown by the following picture:

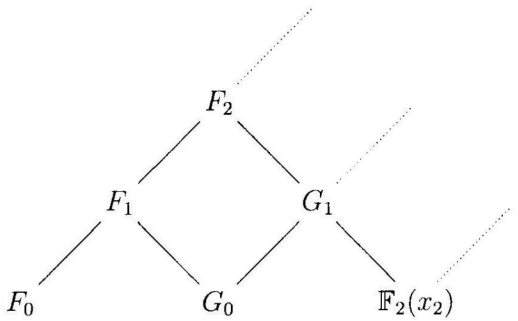


Figure 3.1: F_2

We know that the fields on the same horizontal line in the above picture are isomorphic, i.e., G_1 is $\mathbb{F}_2$-isomorphic to the basic function field under the map $x_1 \mapsto x,\ x_2 \mapsto y$. Therefore, the only ramified place of G_0 in G_1 is the unique pole of x_1 and all other places of G_0 are unramified in G_1. Note that since the rational places of F_i with $i \geq 1$ lie above the rational places of F_{i-1}, to find $N(F_i)$ we consider only the rational extensions of the rational places of F_{i-1}. Now we want to first find the rational places of F_2. We know that the rational places of F_1 are P, Q_i, and R_i for $i = 1, 2$ (see Figure 2.1). Firstly, consider the places Q_1, Q_2, and R_1. Since the valuation $v(x_1^3 + x_1) > 0$ at these places, by Lemma 2.4, each of these places is unramified in F_2 and each has two distinct rational extensions in F_2. Next, consider the places P and R_2. Let Q, R be places of F_2 such that $Q|P$ and $R|R_2$, and $Q' := Q \cap G_1$.

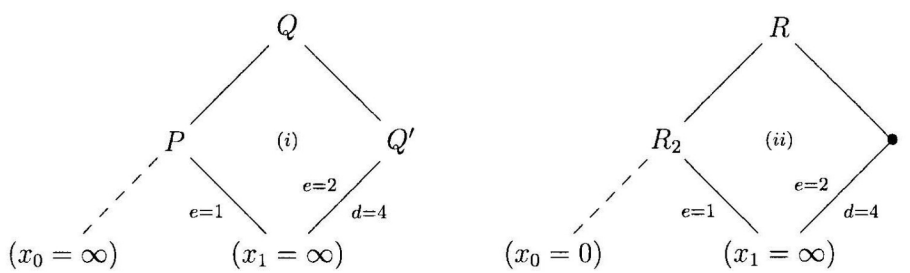


Figure 3.2:

By applying Abhyankar's Lemma 1.3 in the above pictures in (i) and (ii), we can easily infer that P and R_2 are ramified in F_2. Therefore, each of the places P and R_2 has only one rational extension in F_2. Notice that Q is unramified over G_1 by the same lemma. Next, we want to find the different exponent of $Q|P$. By applying the transitivity of the different exponent 1.4 in (i), we get

$$d(Q|(x_1 = \infty)) = e(Q|P)d(P|(x_1 = \infty)) + d(Q|P) = d(Q|P). \tag{3.3}$$

On the other hand we have

$$d(Q|(x_1=\infty)) = e(Q|Q')d(Q'|(x_1=\infty)) + d(Q|Q') = 1\cdot 4 + 0 = 4. \tag{3.4}$$

By combining both of the above equations (3.3) and (3.4), we obtain $d(Q|P) = 4$. Similarly, we get the different exponent of R over R_2, which is $d(R|R_2) = 4$.

Now if we summarize, then we get the following table. In that table S denotes any rational place of F_1 and S' is a place of F_2 lying above S and d denotes the different exponent $d(S'|S)$ (any empty entry of the column of d means that different exponent is zero).

F_1	$\mathbb{F}_2(x_0)$	$\mathbb{F}_2(x_1)$	F_2	d
S	$(x_0=\infty)$	$(x_1=\infty)$	ramified, 1 ext.	4
	$(x_0=1)$	$(x_1=0)$	unram., 2 ext.	
		$(x_1=1)$	unram., 2 ext.	
	$(x_0=0)$	$(x_1=1)$	unram., 2 ext.	
		$(x_1=\infty)$	ramified, 1 ext.	4

Consequently, there are totally 8 rational places of F_2 i.e., $N(F_2) = 8$. To find the genus of F_2, first we need the following lemma.

Lemma 3.1. *Suppose that all rational places of F_0 have only rational extensions in F_{n-1} with $n > 1$. Then all non-rational places of F_{n-1} are unramified in F_n.*

Proof. Let P be a place of $\mathbb{P}_{F_{n-1}}$ with $\deg P > 0$ and Q be an extension of P in F_n. Set $P_i := Q \cap F_i$ and $Q_i := Q \cap G_i$ for $0 \le i \le n-1$. All are shown as follows:

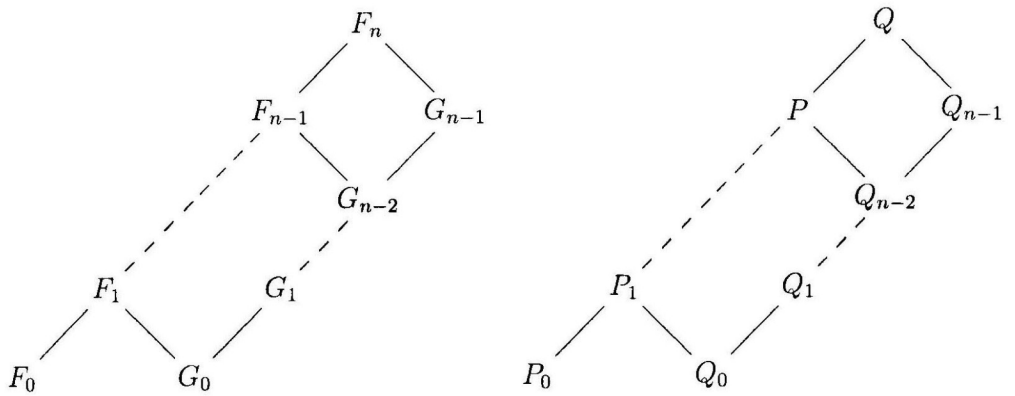


Figure 3.3:

Since P is non-rational, P_1 is also non-rational by our assumption. By Lemma 2.5, Q_0 and Q_1 are also non-rational and $e(P_1|Q_0) = e(Q_1|Q_0) = 1$. Then inductively we see that in the base of the pyramid all ramification indices are 1, and so by Abhyankar's Lemma, we get the desired result. □

Now from the above lemma, it is clear that all non-rational places of F_1 are unramified in F_2, and so they do not contribute to the genus of F_2. Then by using the Hurwitz Genus Formula 1.5, we obtain

$$\begin{aligned} 2g(F_2) - 2 &= [F_2 : F_1](2.g(F_1) - 2) + \deg Diff(F_2/F_1) \\ &= 2 \cdot (2 \cdot 1 - 2) + 4 + 4 = 8, \end{aligned}$$

which gives $g(F_2) = 5$.

Now for simplicity, we introduce a new notation and a proposition which will be useful in the next steps.

Definition 3.2. Let $\mathcal{F} = (F_0, F_1, \ldots)$ be a recursively defined tower of function fields over $\mathbb{F}_q$ such that $F_0 = \mathbb{F}_q(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ for $i \geq 0$. Assume that P is a rational place of F_n for $n \geq 0$ with the restrictions $(x_i = k_i) := P \cap \mathbb{F}_q(x_i)$ for $0 \leq i \leq n$, then $T(P) := (k_0, k_1, \ldots, k_n)$ is called the *tuple* of P.

Proposition 3.3. *Suppose that $\mathcal{F} = (F_0, F_1, \ldots)$ is the tower of function fields over $\mathbb{F}_2$ which is defined by the polynomial (3.1). Let P be a rational place of F_n (for $n \geq 0$) with the tuple $T(P) = (k_0, k_1, \ldots, k_n)$. Then we have*

(a) *For $i \geq 0$,*

- *if $k_i = \infty$, then $k_{i+1} = k_{i+2} = \ldots = k_n = \infty$,*
- *if $k_i = 1$, then $k_{i+1} = 0$ or 1,*
- *if $k_i = 0$, then $k_{i+1} = 1$ or ∞.*

(b) *If $k_n = 0$, then there are two places P_1 and P_2 of F_{n+1} lying above P with*

$$\begin{aligned} T(P_1) &= (k_0, k_1, \ldots, 0, 1) \quad \text{and} \\ T(P_2) &= (k_0, k_1, \ldots, 0, \infty). \end{aligned}$$

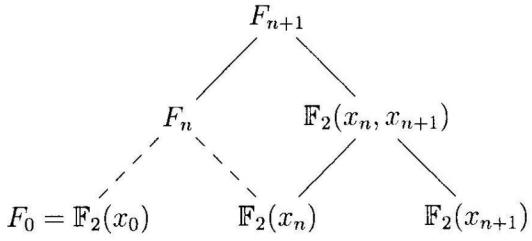
(c) *If $k_n = 1$, then there are two places Q_1 and Q_2 of F_{n+1} lying above P with*

$$\begin{aligned} T(Q_1) &= (k_0, k_1, \ldots, 1, 1) \quad \text{and} \\ T(Q_2) &= (k_0, k_1, \ldots, 1, 0). \end{aligned}$$

(d) *In the case that $T(P) = (\infty, \infty, \ldots, \infty)$ (with $n \geq 0$) or $T(P) = (0, \infty, \ldots, \infty)$ (with $n \geq 1$), P is ramified in F_{n+1} and if P' is a place of F_{n+1} above P, then the different exponent of P' over P is $d(P'|P) = 4$.*

Proof. (*a*) Since $\mathbb{F}_2(x_i, x_{i+1})$ is isomorphic to the basic function field F for all $i \geq 0$, the results in (*a*) immediately follow.

(*b*) We have $k_{n+1} = 0$ or ∞ by (*a*). As by definition, each place clearly has a unique tuple and P has at most two extensions, the result follows (see the following pictures).



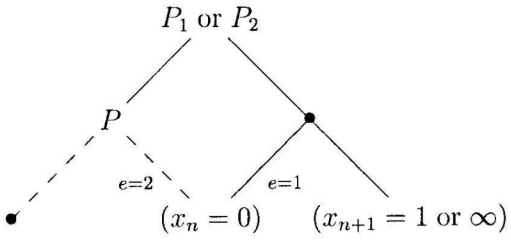


Figure 3.4:

(*c*) In the same way with part (*b*).

(*d*) From the definition of the tower $\mathcal{F}$, we know that $F_{n+1} = F_n(x_{n+1}) = F_n(z_{n+1})$ where $z_{n+1}^2 + z_{n+1} = x_n^3 + x_n$ with $z_{n+1} := x_n x_{n+1}$. Firstly, suppose that $T(P) = (\infty, \ldots, \infty)$. Then as P is a pole of x_n in F_n, by Theorem 1.6 $m_P = 3$, and hence P is ramified in F_{n+1} and $d(P'|P) = 4$.
Now consider the case when $T(P) = (0, \infty, \ldots, \infty)$. Let $Q = P \cap G_{n-1}$ and $Q' = P' \cap G_n$ be the restriction of P (resp., P') to G_{n-1} (resp., G_n) as shown in the following picture;

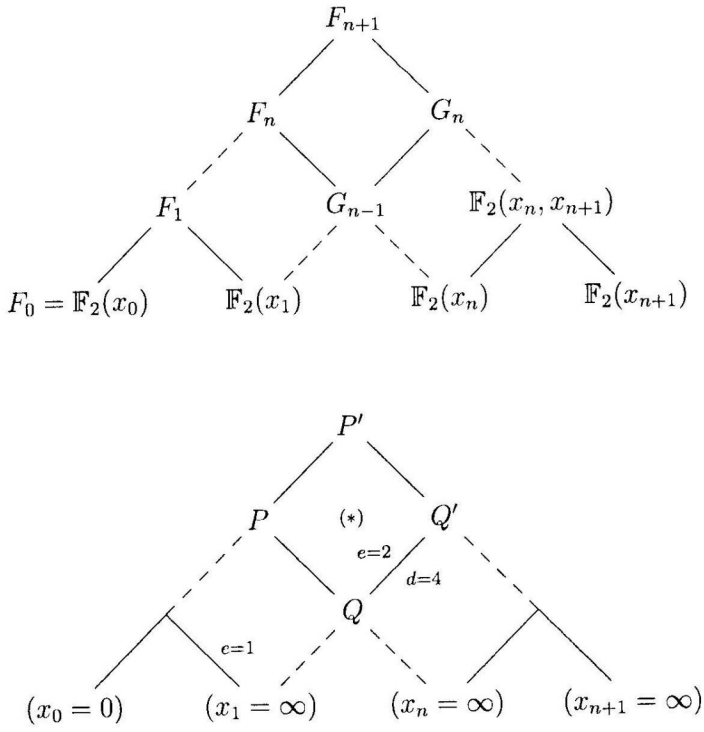


Figure 3.5:

Notice that $T(Q) = (\infty, \infty, \ldots, \infty)$. Therefore, as we have already seen, Q is ramified in G_n and $d(Q'|Q) = 4$. We know that $(x_1 = \infty)$ is unramified in F_1, and so by Abhyankar's Lemma we get $e(P|Q) = e(P'|Q') = 1$ and $e(P'|P) = 2$. To find the different exponent of P' over P, we apply the transitivity of the different exponent in (*);

$$d(P'|Q) = e(P'|P)d(P|Q) + d(P'|P) = 2 \cdot 0 + d(P'|P) = d(P'|P) \tag{3.5}$$

On the other hand we have

$$d(P'|Q) = e(P'|Q')d(Q'|Q) + d(P'|Q') = 1 \cdot 4 + 0 = 4 \tag{3.6}$$

Then by combining the above equations (3.5) and (3.6), we obtain $d(P'|P) = 4$. □

Next, we shall find the rational places and the genus of F_3 which is given by the equation

$$z_3^2 + z_3 = x_2^3 + x_2 \quad \text{where} \quad z_3 := x_2 x_3$$

and shown as follows;

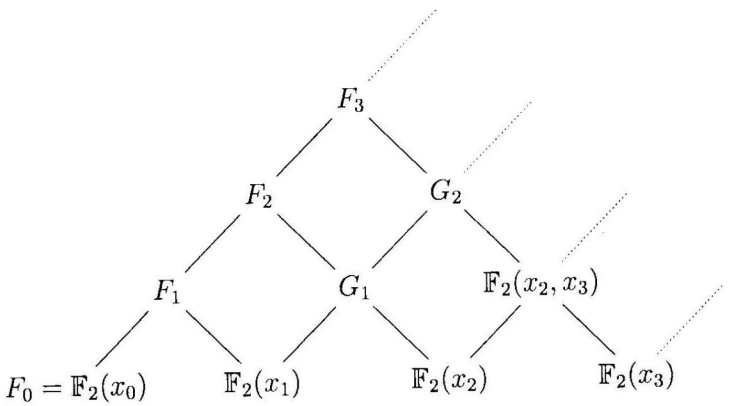


Figure 3.6:

We know that to find the rational places of F_3, it is enough to consider just the rational extensions of the rational places of F_2. Let P be a rational place of F_2. Then by using Proposition 3.3(a), we can write all possibilities for the tuple of P, i.e, $T(P)$ as follows:

(1) $(0,1,0)$, (3) $(1,0,1)$, (6) $(0,\infty,\infty)$,

(2) $(0,1,1)$, (4) $(1,1,1)$, (7) $(1,0,\infty)$,

(5) $(1,1,0)$, (8) (∞,∞,∞).

In fact, we know that $N(F_2) = 8$, and so these are all the possibilities for $T(P)$. Note that for each tuple, there may be more than one place, but in this case there is just one place for each tuple as seen above.

By Proposition 3.3(b) and (c), in each case $1,2,3,4,5$ the place P splits in F_3; that is, it is unramified and it has two distinct rational extensions in F_3. Therefore, we obtain $5 \cdot 2 = 10$ rational places of F_3. By the same proposition, we know that in the cases 6 and 8 the place P is ramified in F_3, and if $P' \in \mathbb{P}_{F_3}$ lies above P, then the different exponent $d(P'|P) = 4$. Hence, we have already got $10 + 1 + 1 = 12$ rational places of F_3. For the remaining case i.e., when P has the tuple $(1,0,\infty)$, we need the following picture. First let $Q := P \cap G_1$ be the restriction of P to the field G_1, and $P' \in \mathbb{P}_{F_3}$ be a place above P. The numbers on the picture show the corresponding ramification index and the numbers written in [.] show the corresponding different exponent. From now on, we will frequently write in that way.

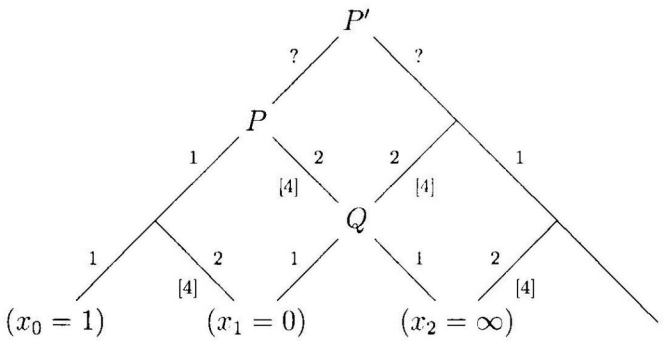


Figure 3.7:

By applying Abhyankar's Lemma in the above picture, we see that Q is ramified in the both fields F_2 and G_2. Hence, we cannot apply this lemma to find the ramification index $e(P'|P)$. Thus, it is not easy to find that index and the different exponent P' over P. We know that $F_3 = F_2(z_3)$ is an Artin Schreier extension of F_2 with the polynomial $T^2 + T + x_2^3 + x_2$. Hence, if we can find an element $u \in F_2$ such that $v_P(x_2^3 + x_2 + u^2 + u) = -m < 0$ where m is relatively prime with 2, then P is ramified, otherwise it is unramified in F_3 by Theorem 1.6. To find such a u, we will use *P-adic power series.*

Definition 3.4. Let P be a place of a function field F/K. The completion of F with respect to the valuation v_P is called the *P-adic completion* of F. We denote this completion by $\hat{F}_P$ and the valuation of $\hat{F}_P$ by v_p.

Theorem 3.5. *Let $P \in \mathbb{P}_F$ be a place of degree one and $t \in F$ be a P-prime element. Then any element $z \in \hat{F}_P$ has a unique representation of the form*

$$z = \sum_{i=n}^{\infty} a_i t^i \quad \textit{with} \quad n \in \mathbb{Z} \quad \textit{and} \quad a_i \in K.$$

This representation is called the P-adic power series expansion of z with respect to t.

Proof. See [1, p.164]. □

Now we return to the problem mentioned above, i.e., how to find the element u. We have (see Figure 3.7)

- $e(P|(x_0 = 1)) = 1$, so $v_P(x_0 + 1) = 1$, whence $t := x_0 + 1$ is a P-prime element,
- $e(P|(x_1 = 0)) = 2$, so $v_P(x_1) = 2$, and
- $e(P|(x_2 = \infty)) = 2$, so $v_P(x_2) = -2$.

We need to find the P-adic power series expansion of x_2 with respect to t. To do this, we will firstly find the P-adic power series expansion of x_1 with respect to t, where

$$x_1 = \sum_{i=n}^{\infty} a_i t^i \quad \text{with} \quad a_i \in \mathbb{F}_2,\ n = 2, \quad \text{and} \quad a_2 = 1 \quad \text{since} \quad v_P(x_1) = 2.$$

Notice that a_i is 0 or 1 and $a_i^2 = a_i$ for all $i > 2$. We have

$$x_1^2 x_0 + x_1 = x_0^2 + 1 = (x_0 + 1)^2 = t^2.$$

Inserting $x_1 = \sum_{i=2}^{\infty} a_i t^i$ and $x_0 = t+1$ into the above equation gives

$$\begin{aligned} \sum_{i=2}^{\infty} a_i t^{2i}(t+1) + \sum_{i=2}^{\infty} a_i t^i &= \sum_{i=2}^{\infty} a_i t^{2i+1} + \sum_{i=2}^{\infty} a_i t^{2i} + \sum_{i=2}^{\infty} a_i t^i \\ &= t^5 + a_3 t^7 + a_4 t^9 + \cdots + t^4 + a_3 t^6 + a_4 t^8 + \cdots \\ &\quad + t^2 + a_3 t^3 + a_4 t^4 + a_5 t^5 + a_6 t^6 + a_7 t^7 + a_8 t^8 + \cdots \\ &= t^2 \end{aligned}$$

By comparing the coefficients of t^i of the both sides of the above equality, we get

- $a_3 = a_6 = a_7 = 0$,
- $a_4 = a_5 = a_8 = 1$, etc.

Therefore, $x_1 = t^2 + t^4 + t^5 + t^8 +$ *higher powers of* t. Now we have

$$x_2 = \sum_{i=n}^{\infty} b_i t^i \quad \text{with} \quad b_i \in \mathbb{F}_2, \quad n = -2, \quad \text{and} \quad b_{-2} = 1 \quad \text{since} \quad v_P(x_2) = -2.$$

We want to find b_i for $i > -2$.

If we put $x_1 = t^2 + t^4 + t^5 + t^8 + \cdots$ and $x_2 = \sum_{i=-2}^{\infty} b_i t^i$ in the equation

$$x_2^2 x_1 + x_2 = x_1^2 + 1, \quad \text{then we obtain}$$

$$\begin{aligned} &\sum_{i=-2}^{\infty} b_i t^{2i}(t^2 + t^4 + t^5 + t^8 + \cdots) + \sum_{i=-2}^{\infty} b_i t^i = t^{-2} + 1 + t + t^4 + \cdots + b_{-1} + b_{-1} t^2 + b_{-1} t^3 \\ &+ b_{-1} t^6 + \cdots + b_0 t^2 + b_0 t^4 + b_0 t^5 + \cdots + b_1 t^4 + b_1 t^6 + \cdots + b_2 t^6 + \cdots \\ &+ t^{-2} + b_{-1} t^{-1} + b_0 + b_1 t + b_2 t^2 + b_3 t^3 + b_4 t^4 + b_5 t^5 + \cdots \\ &= 1 + t^4 + t^8 + t^{10} + \ldots \end{aligned}$$

By comparing the coefficients of t^i of the both sides of the above equality, we get

- $b_{-1} = b_0 = b_2 = b_3 = 0$
- $b_1 = b_4 = 1$, etc.

Thus, $x_2 = t^{-2} + t + t^4 +$ *higher powers of* t. Now

$$\begin{aligned} x_2^3 = x_2^2.x_2 &= (t^{-4} + t^2 + \cdots).(t^{-2} + t + t^4 + \cdots) \\ &= t^{-6} + t^{-3} + 1 + \cdots + 1 + t^3 + \cdots \\ &= t^{-6} + t^{-3} + t^3 + \cdots \end{aligned}$$

Let $u := t^{-3} + t^{-1}$. Then

$$\begin{aligned} v_P(x_2^3 + x_2 + u^2 + u) &= v_P(t^{-6} + t^{-3} + t^3 + \cdots + t^{-2} + t \cdots + t^{-6} + t^{-2} + t^{-3} + t^{-1}) \\ &= v_P(\ (\textit{positive powers of } t) + t^{-1}) = -1. \end{aligned}$$

This gives us $m_P = 1 > 0$, and so by Theorem 1.6 P is ramified in F_3, and the different exponent is

$$d(P'|P) = (p-1) \cdot (m_P + 1) = 1 \cdot 2 = 2.$$

Consequently, we have totally $12 + 1 = 13$ rational places of F_3, i.e., $N(F_3) = 13$. Moreover, by Lemma 3.1, all non-rational places of F_2 are clearly unramified in F_3. Thus, the Hurwitz Genus Formula for the extension F_3/F_2 gives

$$\begin{aligned} 2 \cdot g(F_3) - 2 &= [F_3 : F_2] \cdot (2 \cdot g(F_2) - 2) + degDiff(F_3/F_2) \\ &= 2 \cdot (2 \cdot 5 - 2) + 2 \cdot 4 + 2 = 26, \end{aligned}$$

and so $g(F_3) = 14$.

Next, we move on to the fourth step F_4, which is given by the equation

$$z_4^2 + z_4 = x_3^3 + x_3 \quad \text{where} \quad z_4 := x_3 x_4.$$

The picture for F_4 is as follows:

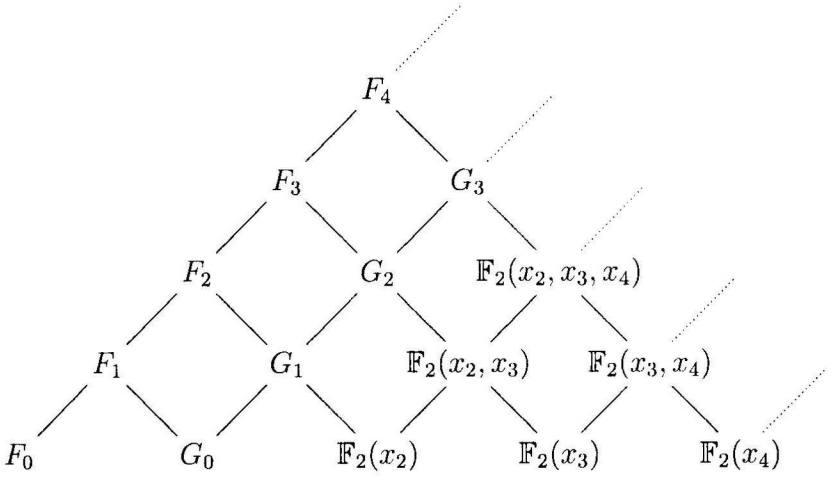


Figure 3.8:

We want to find the number of rational places and the genus of F_4. Since to find the rational places it is enough to consider the rational extensions of the rational places of F_3, we take a rational place P of F_3. Then by using Proposition 3.3 and by looking at the tuples of the rational places of F_2, which we know from the previous step, we can write all possible tuples of P. In other words, we get all distinct tuples of the rational places of F_3. Our tuples are as follows:

(1) $(0,1,0,1)$, (5) $(1,0,1,0)$, (11) $(0,\infty,\infty,\infty)$,

(2) $(0,1,0,\infty)$, (6) $(1,0,1,1)$, (12) $(1,0,\infty,\infty)$,

(3) $(0,1,1,0)$, (7) $(1,1,1,0)$, (13) $(\infty,\infty,\infty,\infty)$.

(4) $(0,1,1,1)$, (8) $(1,1,1,1)$,

(9) $(1,1,0,1)$,

(10) $(1,1,0,\infty)$,

Since F_3 has exactly 13 rational places, these are the all cases. We know that by our nice Proposition 3.3, in all the cases except for the tuples ending with ∞, the place P is unramified and it has two rational extensions in F_4. Hence, from that cases, we obtain $8 \cdot 2 = 16$ rational places of F_4. Next, by the same proposition, in the cases 11, 13 we see that P is ramified in F_4 and if $P' \in \mathbb{P}_F$ with $P'|P$, then the different exponent $d(P'|P) = 4$. Therefore, now we have $16 + 1 + 1 = 18$ rational places of F_4. We are left with the cases 2, 10, 12. First we consider the cases 2 and 10. Let P' be a

place of F_4 lying above P. Suppose that Q, Q' are the restrictions of P, P' to G_2, G_3, respectively. Then by applying Abhyankar's Lemma, we have the following situation:

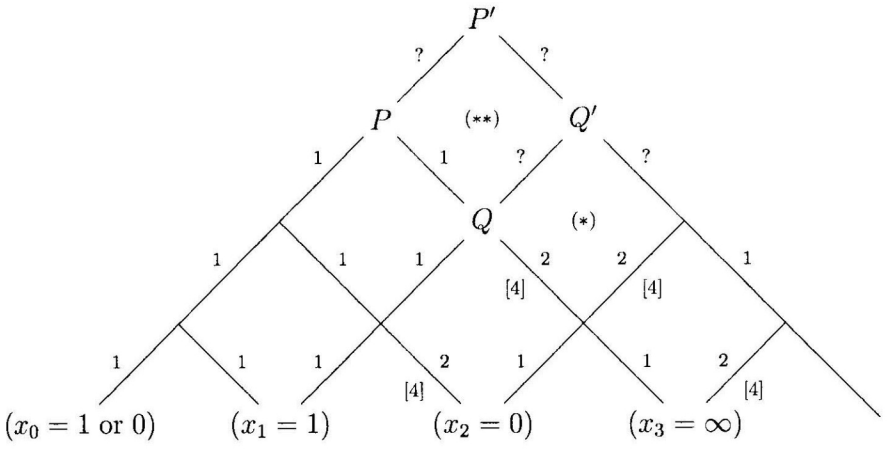


Figure 3.9:

We observe that Abhyankar's Lemma cannot be used in (*). By using the ramifications indices, we get

$$v_Q(x_3) = -2, \quad v_Q(x_2) = 2 \quad \text{and}$$
$$v_Q(x_1 + 1) = 1, \quad \text{which implies that } x_1 + 1 \text{ is a } Q\text{-prime element.}$$

Notice that we have the same situation as we handled during the studying of F_3 (see p.17). Moreover, we know that as F_3 and G_3 are on the same horizontal line, they are isomorphic (under the map $x_i \to x_{i+1}$ for $i = 0, 1, 2, 3$). Hence, if we apply P-adic power series method 3.5, we see that Q is ramified in G_3 and the different exponent $d(Q'|Q) = 2$. Now by applying Abhyankar's Lemma and the transitivity of the different exponent in (**), we can easily obtain that P is ramified in F_4 and $d(P'|P) = 2$. Note that we are working on the cases 2 and 10, and so we have for each case, one rational extension of P with the different exponent 2. Now we have $18 + 1 + 1 = 20$ rational places of F_4.

Our last case is 12, where the tuple of P is $(1, 0, \infty, \infty)$. Let us use the same notations as we have already used, which are P', Q and Q' with the same definitions. We have the following situation (see Figure 3.7):

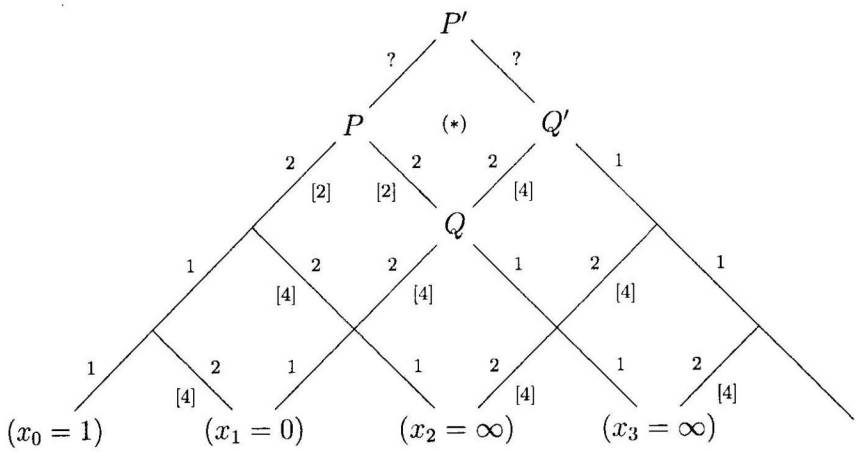


Figure 3.10:

Applying Abhyankar's Lemma in the above picture gives that Q is ramified in both of the fields F_3 and G_3. Therefore, this lemma is not applicable in (*). Further, since it is not easy to find a P-prime element, we do not apply the way of P-adic power series, which we used before. First we claim that P is ramified. To prove this, we apply the transitivity of the different exponent in (*);

$$\begin{aligned} d(P'|Q) &= e(P'|P)d(P|Q) + d(P'|P) && (3.7)\\ &= 2 \cdot e(P'|P) + d(P'|P) && (3.8) \end{aligned}$$

On the other hand we have

$$\begin{aligned} d(P'|Q) &= e(P'|Q')d(Q'|Q) + d(P'|Q') && (3.9)\\ &= 4 \cdot e(P'|Q') + d(P'|Q') && (3.10) \end{aligned}$$

By using the fact that $e(P'|P) = e(P'|Q')$ and by combining the above equations, we obtain that

$$d(P'|P) = 2e(P'|P) + d(P'|Q') > 0 \quad \text{since } e(P'|P) > 0.$$

Therefore, P must be ramified, otherwise $d(P'|P) = 0$, a contradiction. But, we still do not know the different exponent $d(P'|P)$. Thus, we will use another method, which also will be useful for the next steps. First we need the following definition.

Definition 3.6. Let F'/F be a Galois extension of algebraic function fields with Galois group $G = Gal(F'/F)$. Consider a place $P \in \mathbb{P}_F$ and an extension P' of P in F'. For any $i \geq -1$, we define the *i-th ramification group* of $P'|P$ by

$$G_i(P'|P) := \{\sigma \in G |\ v_{P'}(\sigma z - z) \geq i + 1 \text{ for all } z \in \mathcal{O}_{P'}\}.$$

Clearly, $G_i(P'|P)$ is a subgroup of G and $G \supseteq G_{-1} \supseteq G_0 \supseteq \ldots \supseteq G_m \supsetneq G_{m+1} = \{id\}$ for some sufficiently large m. For simplicity, we write $G_i := G_i(P'|P)$. Further, the order of the group G_0 is equal to the ramification index $e(P'|P)$ (for the proof of that fact see [1, Theorem 3.8.2]).

Theorem 3.7 (Hilbert's Different Formula). *Consider a Galois extension F'/F of algebraic function fields, a place $P \in \mathbb{P}_F$ and a place $P' \in \mathbb{P}_{F'}$ lying over P. Then the different exponent $d(P'|P)$ is*

$$d(P'|P) = \sum_{i=0}^{\infty} (ord\, G_i(P'|P) - 1).$$

(Note that this is a finite sum, since $G_i(P'|P) = \{id\}$ for large i.)

Proof. See [1, p.136]. □

Proposition 3.8. *Let F'/F be a Galois extension of algebraic function fields with extension degree $[F' : F] = p^2$. Suppose that $F' = F_1F_2$ is the compositum of two intermediate fields $F \subsetneq F_1, F_2 \subsetneq F'$ with $[F_i : F] = p$ for $i = 1, 2$. Let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ be an extension of P, and set $P_i := P' \cap F_i$ for $i = 1, 2$. Assume that $e(P_i|P) = p$ (for $i = 1, 2$), $d(P_1|P) = s(p-1)$ and $d(P_2|P) = t(p-1)$ where s, t are positive integers with $s < t$. Then the following assertions hold:*

(i) $e(P'|P) = p^2$,

(ii) $d(P'|P_2) = d(P_1|P) = s(p-1)$,

(iii) $d(P'|P_1) = (p(t-s)+s)(p-1)$.

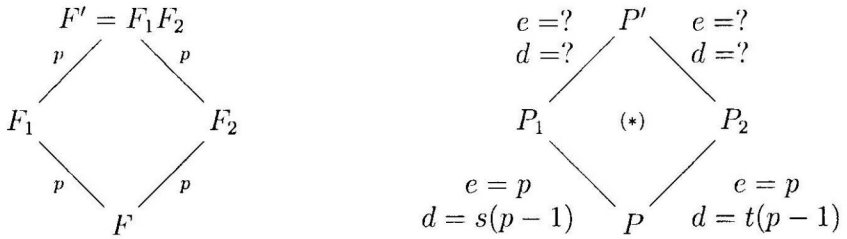


Figure 3.11:

Proof. (i) Clearly, by applying the transitivity of the different exponent in the above picture (*), we see that $e(P'|P) = p^2$, otherwise $e(P'|P_1) = e(P'|P_2) = 1$, and so we get $s = t$, which is a contradiction.

(ii) and (iii) We begin by proving the following claim: Let $G := Gal(F'|F)$ and G_i be the i-th ramification group of P' over P for $i \geq -1$. Then there exist integers r_1, r_2 with $r_2 > r_1 \geq 1$ such that

$$G = G_0 = G_1 = \ldots = G_{r_1-1} \supsetneq G_{r_1} = G_{r_1+1} = \ldots = G_{r_2-1} \supsetneq G_{r_2} = \{id\}. \quad (3.11)$$

To prove this claim, firstly note that since ord $G_0 = e(P'|P) = p^2$, we have $G = G_{-1} = G_0$. Now suppose that

$$G = G_0 = G_1 = \ldots = G_r \supsetneq G_{r+1} = \{id\} \text{ for some } r \geq 0. \quad (3.12)$$

Then by Hilbert's Different Formula 3.7, we get $d(P'|P) = (r+1)(p^2-1)$. Let U be a subgroup of G with ord $U = p$ and denote its fixed field by U'. Let $P_{U'} := P' \cap U'$. Then

$$U = U_0 = U_1 = \ldots = U_r \supsetneq U_{r+1} = \{id\}$$

where U_i denotes the i-th ramification group of $P'|P_{U'}$. Therefore, again by applying Hilbert's Different Formula, we obtain $d(P'|P_{U'}) = (r+1)(p-1)$, which implies that for any extension $P_{U'}$ of P, different exponent is the same by the transitivity of the different exponent for $P'|P_{U'}|P$. But, we have two different extensions of P, namely P_1 and P_2 with distinct different exponents. Thus, (3.12) is not possible.
Therefore, we have (3.11), and so $d(P'|P) = r_1(p^2-1)+(r_2-r_1)(p-1) = (r_1p+r_2)(p-1)$. Moreover, note that since $G \cong Gal(F'/F_1) \times Gal(F'/F_2) \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ (under the map $\sigma \to (\sigma_{|F_1}, \sigma_{|F_2})$), G has $p+1$ distinct subgroups with order p. In fact, this is clear because $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has exactly $p+1$ subgroups with order p, which are

$$H = \{(0,y) : y \in \mathbb{Z}_p\} \text{ and } H_m = \{(x,mx) \in \mathbb{Z}_p \oplus \mathbb{Z}_p : x \in \mathbb{Z}_p\} \text{ for each } m \in \mathbb{Z}_p.$$

Now we can choose a nontrivial subgroup of G in the following ways;

(1) $U := G_{r_1}$. Let U' be the fixed field of U and $P_{U'} := P' \cap U'$. Then the ramification groups of P' over $P_{U'}$ satisfies

$$U_0 = U_1 = \ldots = U_{r_2-1} \supsetneq U_{r_2} = \{id\},$$

and hence $d(P'|P_{U'}) = r_2(p-1)$. Also, by applying the transitivity of the different exponent,

$$d(P'|P) = e(P'|P_{U'})d(P_{U'}|P) + d(P'|P_{U'}),$$

and so we obtain

$$\begin{aligned} d(P_{U'}|P) &= \frac{1}{p}\left[(r_1p + r_2)(p-1) - r_2(p-1)\right] \\ &= \frac{r_1p(p-1)}{p} = r_1(p-1). \end{aligned}$$

(2) $V \subsetneqq G$, but $V \neq G_{r_1}$ with $ord\ V = p$. Notice that G has p distinct such subgroups. Let V' be the fixed field of V and $P_{V'} := P' \cap V'$. Then the ramification groups $V_i := G_i(P'|P_V)$ satisfies

$$V = V_0 = V_1 = \ldots = V_{r_1-1} \supsetneqq V_{r_1} = \{id\},$$

and so $d(P'|P_{V'}) = r_1(p-1)$. Thus, similarly we get

$$\begin{aligned} d(P_{V'}|P) &= \frac{1}{p}\left[(r_1p + r_2)(p-1) - r_1(p-1)\right] \\ &= \frac{1}{p}\left[(r_1p - r_1 + r_2)(p-1)\right] = \left(r_1 + \frac{r_2 - r_1}{p}\right)(p-1). \end{aligned}$$

(Note that we must have $r_2 \equiv r_1 \mod p$.)

We know that by the Fundamental Theorem of Galois Theory, there is a one-to-one correspondence between subfields of F' and subgroups of G. We have seen that there exists a unique subgroup $U \subseteq G$ which yields the different exponent $d(P_{U'}|P) = r_1(p-1)$. Therefore, since $s < t$, we have $s = r_1$, $F_1 = U'$ and $t = r_1 + \frac{r_2 - r_1}{p}$, $F_2 = V'$ for some $V' \neq U'$. All different exponents are shown in the following picture:

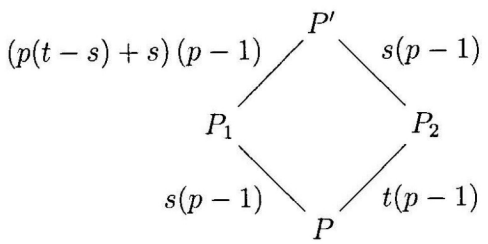


Figure 3.12:

□

Now we return to the problem, which was how to find $d(P'|P)$ in the case that $T(P) = (1, 0, \infty, \infty)$. We have the following situation;

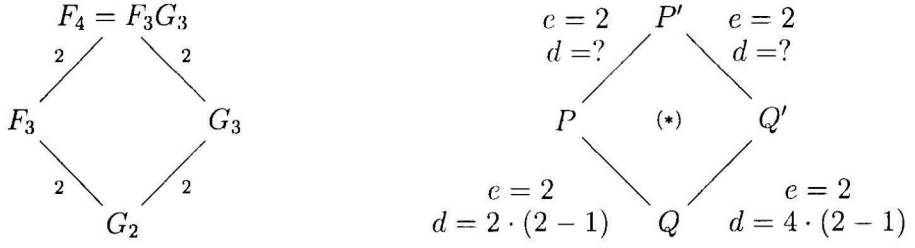


Figure 3.13:

Thus, by Proposition 3.8, we get $d(P'|Q') = 2$, and $d(P'|P) = 6$. Consequently, we have totally $20+1 = 21$ rational places of F_4, i.e., $N(F_4) = 21$. Further, by Lemma 3.1, all non-rational places of F_3 are unramified in F_4. Now we apply the Hurwitz Genus Formula to find the genus of F_4;

$$\begin{aligned} 2 \cdot g(F_4) - 2 &= [F_4 : F_3] \cdot (2 \cdot g(F_3) - 2) + \deg Diff(F_4/F_3) \\ &= 2 \cdot (2 \cdot 14 - 2) + 2 \cdot 4 + 2 \cdot 2 + 6 = 70, \end{aligned}$$

and hence $g(F_4) = 36$.

Before studying the 5^{th} step of the tower $\mathcal{F}$, we put together all conclusions of what we have done so far. That results will be quite useful in the next steps. First we will introduce a new notation.

Definition 3.9. Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a recursively defined tower of function fields over $\mathbb{F}_q$ and Q be a place of F_n for some $n \geq 0$. Suppose that $Q_i := Q \cap F_i$ is the restriction of Q to F_i and the different exponent $d(Q_{i+1}|Q_i) = d_i$ for $0 \leq i \leq n-1$. Then $\Delta(Q) := (d_0, d_1, \ldots d_{n-1})$ is called the *tuple of the different exponents* for Q.

We observe that in the case that F_n/F_{n-1} is a Galois extension, the tuple $\Delta(Q)$ depends only on the place Q_{n-1}.

Lemma 3.10. *Assume that $\mathcal{F} = (F_0, F_1, \ldots)$ is our main tower and P is a rational place of F_n with an extension Q in F_{n+1} for some $n \geq 0$. Then we have the following;*

(a) *Suppose that the tuple of P is $T(P) = (1, 0, \infty, \ldots, \infty)$. Then the tuple of the different exponents for Q is*

$$\Delta(Q) = (0, 0, 2, 6, 6, 6, \ldots, 6).$$

That means; $d_i = 6$ for all $3 \leq i \leq n$.

(b) *Suppose that there is an integer m with $0 < m < n$ such that $k_0 = 1$ or 0, and $k_j = 1$ for $1 \leq j \leq m$, and $k_{m+1} = 0$, $k_{m+2} = \ldots = k_n = \infty$. That is,*

$T(P) = (1, 1, 1, \ldots, 1, 0, \infty, \ldots, \infty)$ *or* $T(P) = (0, 1, 1, \ldots, 1, 0, \infty, \ldots, \infty)$. *Then the tuple of the different exponents for* Q *is*

$$\Delta(Q) = (0, 0, \ldots, 0, 0, 2, 6, 6, \ldots, 6), \quad \textit{i.e.,} \quad d_i = 0 \quad \textit{for all} \quad 0 \leq i \leq m+1.$$

(c) *Suppose that* P *has the tuple* $T(P) = (\ldots, 1, 0, \infty)$. *In other words;* $k_i = 1$ *or* 0 *for all* $0 \leq i \leq n-3$ *and* $k_{n-2} = 1$, $k_{n-1} = 0$, *and* $k_n = \infty$. *Then we have*

$$\Delta(Q) = (0, \ldots, 0, 2), \quad \textit{i.e,} \quad d_i = 0 \quad \textit{for all} \quad 0 \leq i \leq n-1 \quad \textit{and} \quad d_n = 2.$$

Proof. (*a*) We know that it is true for $n \leq 4$ (see Figure 3.10). So we consider the case $n \geq 5$. Let P_4 be the restriction of P to F_4, and $Q_k := Q \cap G_k$ for all $0 \leq k \leq n$. Then we have the following situation:

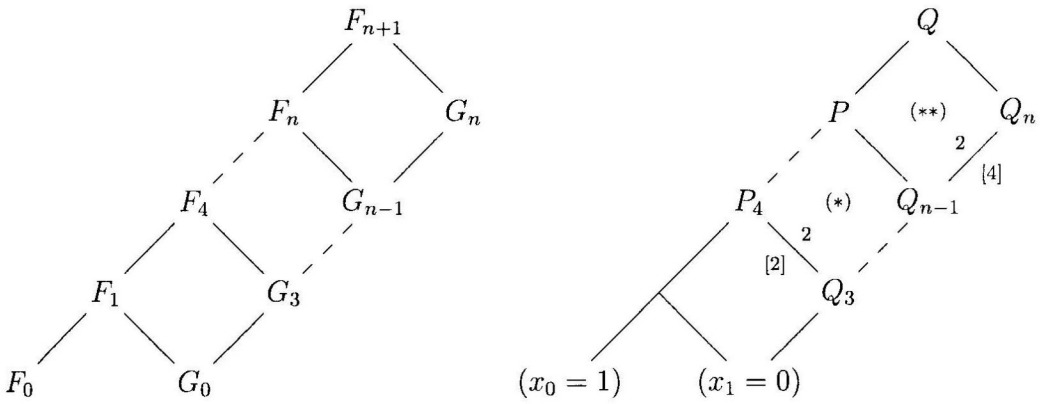


Figure 3.14: $T(P) = (1, 0, \infty, \ldots, \infty)$

Since $T(Q_{n-1}) = (0, \infty, \ldots, \infty)$, by Proposition 3.3, we know that $\Delta(Q_n) = (0, 4, 4, \ldots, 4)$, which implies that $d(Q_k|Q_{k-1}) = 4$ for $k \geq 2$. Further, we know that $d(P_4|Q_3) = 2$ (see p.26). Hence, by applying Proposition 3.8 in (*) then in (**) for each $n \geq 0$, we get inductively $d(Q|Q_n) = 2$, and $d(Q|P) = 6$.

(*b*) Let $P_{m+i} := Q \cap F_{m+i}$, and $Q_{m+i} := Q \cap \mathbb{F}_2(x_m, x_{m+1}, \ldots, x_{m+i})$ for $0 \leq i \leq n-m+1$. All are shown by the following pictures:

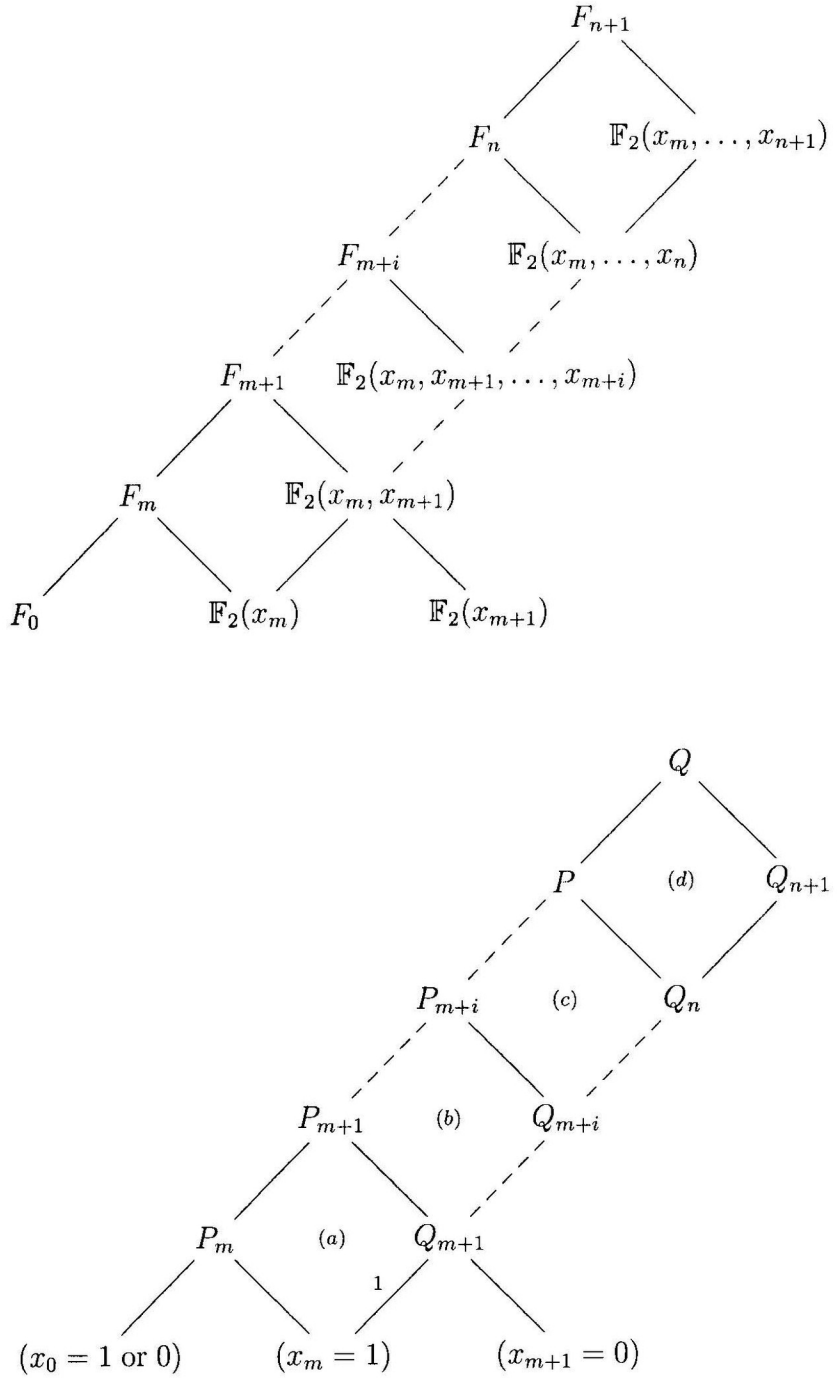


Figure 3.15: $T(P) = (1, 1, \ldots, 1, 0, \infty, \ldots, \infty)$ or $(0, 1, 1, \ldots, 1, 0, \infty, \ldots, \infty)$

As $T(Q_n) = (1, 0, \infty, \ldots, \infty)$, we have seen that $\Delta(Q_{n+1}) = (0, 0, 2, 6, \ldots, 6)$ by part (a). Next, we claim that the ramification index $e(P_m|(x_0 = k_0)) = 1$ for $k_0 = 0$ or 1. Indeed, as $(x_{j+1} = 1)$ is unramified in the fields $\mathbb{F}_2(x_j, x_{j+1})$ and $\mathbb{F}_2(x_{j+1}, x_{j+2})$ for all $j \geq 0$, in particular for all $1 \leq j \leq m$, in the base of the

pyramid all ramification indices are 1. By using Abhyankar's Lemma, we climb up the pyramid until the m^{th} step and we always obtain ramification indices as 1. Thus, the claim follows, and so $d_j = 0$ for all $0 \leq j \leq m-1$. Moreover, we get similarly the ramification index $e(P_m|(x_m = 1)) = 1$. Now by applying Abhyankar's Lemma sequentially in (a), (b), (c), (d), we see that

$$e(P_{m+i}|Q_{m+i}) = 1 \quad \text{for all} \quad 0 \leq i \leq n-m+1,$$

and hence the result follows by the transitivity of the different exponent.

(c) From the following picture, we see that in any case whether there is an $m > 0$ with $k_m = 0$, $k_{m+1} = 1$ or not we have always the same result. That is $d_n = d(Q|P) = 2$ and $d_i = 0$ for all $0 \leq i \leq n-1$. We have the following situation:

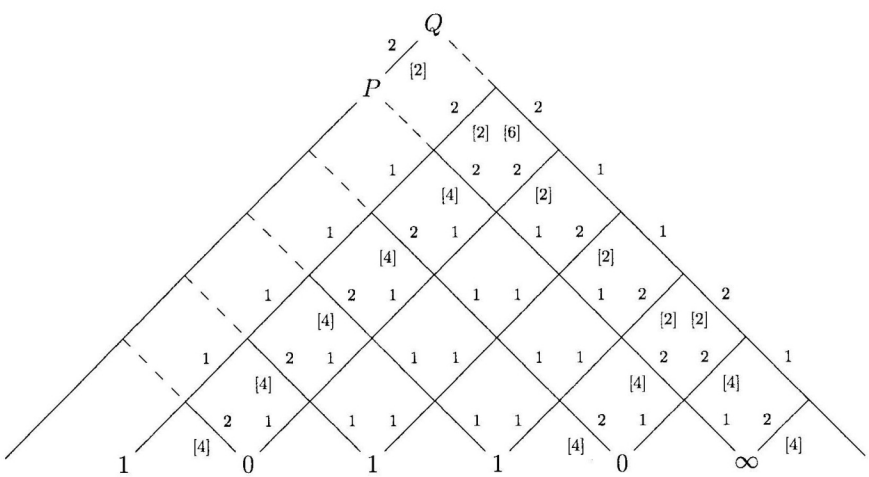


Figure 3.16: $T(P) = (\ldots, 0, \infty)$

□

Now we are ready to treat the 5^{th} step, F_5. As usual, to find the rational places of F_5, we consider the rational extensions of the rational places of F_4. We take a rational place P of F_4. Knowing the tuples of the rational places of F_3 and by using Proposition 3.3, we can write all possible tuples of P, which are as follows:

(1) $(0,1,0,1,0)$, (6) $(1,0,1,0,1)$, (14) $(0,1,0,\infty,\infty)$,

(2) $(0,1,0,1,1)$, (7) $(1,0,1,1,0)$, (15) $(0,1,1,0,\infty)$,

(3) $(0,1,1,0,1)$, (8) $(1,0,1,1,1)$, (16) $(1,0,1,0,\infty)$,

(4) $(0,1,1,1,1)$, (9) $(1,1,1,0,1)$, (17) $(1,1,1,0,\infty)$,

(5) $(0,1,1,1,0)$, (10) $(1,1,1,1,0)$, (18) $(1,1,0,\infty,\infty)$,

(11) $(1,1,1,1,1)$, (19) $(0,\infty,\infty,\infty,\infty)$,

(12) $(1,1,0,1,0)$, (20) $(1,0,\infty,\infty,\infty)$

(13) $(1,1,0,1,1)$, (21) $(\infty,\infty,\infty,\infty,\infty)$.

These are all possibilities because $N(F_4) = 21$.

By Proposition 3.3, in the cases $1 - 13$, P is unramified and it has 2 rational extensions for each of these cases. That is, we obtain $13 \cdot 2 = 26$ rational places of F_5. In the remaining cases, by Proposition 3.3 and Lemma 3.10, P is ramified and the tuple of the different exponents for P are respectively as follows; (for brevity, we shall use P_i for the extension of P in F_{n+1}, for each case $14 \leq i \leq 21$.)

$$\Delta(P_{14}) = (0,0,0,2,6),$$
$$\Delta(P_{15}) = \Delta(P_{16}) = \Delta(P_{17}) = (0,0,0,0,2),$$
$$\Delta(P_{18}) = (0,0,0,2,6), \qquad \Delta(P_{19}) = (0,4,4,4,4),$$
$$\Delta(P_{20}) = (0,0,2,6,6), \qquad \Delta(P_{21}) = (4,4,4,4,4).$$

Hence, we get totally $26 + 8 \cdot 1 = 34$ rational places of F_5, i.e., $N(F_5) = 34$. As usual by applying Lemma 3.1, we see that all non-rational places of F_4 are unramified in F_5. Now to compute the genus of F_5, we apply the Hurwitz Genus Formula and the tuples of different exponents for P given above;

$$\begin{aligned} 2 \cdot g(F_5) - 2 &= [F_5 : F_4] \cdot (2 \cdot g(F_4) - 2) + \deg\ Diff(F_5/F_4) \\ &= 2 \cdot (2 \cdot 36 - 2) + 2 \cdot 4 + 3 \cdot 2 + 3 \cdot 6 \\ &= 2 \cdot 70 + 32 = 172\,, \end{aligned}$$

and so $g(F_5) = 87$.

We now want to investigate the 6^{th} step, F_6. This step is handled similarly, but it is harder. We need to find all possible tuples for a rational place of F_5. Since there are lots of tuples it is not easy to write all of them. We have $5, 8, 8$ tuples written for the previous step ending with $0, 1, \infty$, respectively. We know that by Proposition 3.3,

$$k_n = 0 \Rightarrow k_{n+1} = 1 \text{ or } \infty,$$
$$k_n = 1 \Rightarrow k_{n+1} = 0 \text{ or } 1,$$
$$k_n = \infty \Rightarrow k_{n+1} = \infty .$$

Hence, we get $5+8 = 13$ tuples ending with 1, and 8 tuples ending with 0 and $8+5 = 13$ tuples ending with ∞ of the rational places of F_5. These are all the tuples since we know that $N(F_5) = 34$. From the same proposition, we infer also that all rational places with tuples ending with 0 or 1 split in F_6. Hence, we obtain $2 \cdot (13 + 8) = 42$ rational places of F_6. Since we do not know the extensions of the places with tuples ending with ∞, we need to write all such tuples explicitly so that we can treat each of them separately and find the different exponent. We write them by looking at the tuples written for the 5^{th} step. All are as follows:

(1) $(0, 1, 0, \infty, \infty, \infty)$, (9) $(0, 1, 0, 1, 0, \infty)$,

(2) $(0, 1, 1, 0, \infty, \infty)$, (10) $(0, 1, 1, 1, 0, \infty)$,

(3) $(1, 0, 1, 0, \infty, \infty)$, (11) $(1, 0, 1, 1, 0, \infty)$,

(4) $(1, 1, 1, 0, \infty, \infty)$, (12) $(1, 1, 1, 1, 0, \infty)$,

(5) $(1, 1, 0, \infty, \infty, \infty)$, (13) $(1, 1, 0, 1, 0, \infty)$.

(6) $(0, \infty, \infty, \infty, \infty, \infty)$,

(7) $(1, 0, \infty, \infty, \infty, \infty)$,

(8) $(\infty, \infty, \infty, \infty, \infty, \infty)$,

Now by Proposition 3.3 and Lemma 3.10, we can write the following tuples of different exponents (we use P_i to refer the extension of P in the i^{th} case in above).

$$\Delta(P_1) = \Delta(P_5) = (0, 0, 0, 2, 6, 6), \qquad \Delta(P_2) = \Delta(P_4) = (0, 0, 0, 0, 2, 6),$$
$$\Delta(P_6) = (0, 4, 4, 4, 4, 4), \qquad \Delta(P_7) = (0, 0, 2, 6, 6, 6), \qquad \Delta(P_8) = (4, 4, 4, 4, 4, 4),$$
$$\Delta(P_9) = \Delta(P_{10}) = \Delta(P_{11}) = \Delta(P_{12}) = \Delta(P_{13}) = (0, 0, 0, 0, 0, 2).$$

For the remaining case, namely (3), where $T(P) = (1, 0, 1, 0, \infty, \infty)$ we need to draw the required picture.

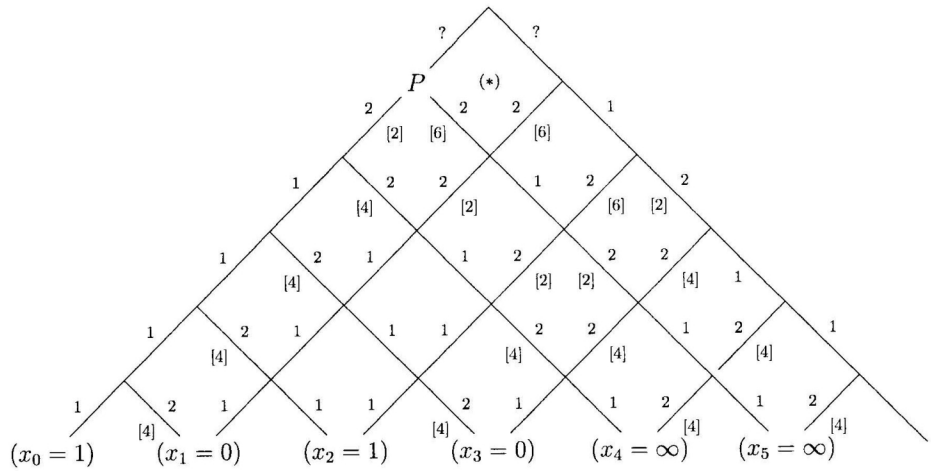


Figure 3.17: $T(P) = (1, 0, 1, 0, \infty, \infty)$

In the above picture, until the region of (*), we know the different exponents and the ramification indices. But in (*), none of the methods that we used until now are applicable. We may apply the method of P-adic Power expansion, but this is not easy because for this, we need to find a prime element for the place P and this is rather difficult. Indeed, even if we find a prime element, we need to do some more calculations to find an element u so that we can apply Theorem 1.6. Hence, we left it as $\Delta(P_3) = (0, 0, 0, 0, 2, ?)$.

Consequently, we have seen that for the cases $1 - 13$, except in the case 3, the place P is ramified in F_6. Hence, we obtain $42 + 12 = 54$ rational places of F_6. Thus,

$$\begin{aligned} N(F_6) &= 54 \quad \text{if } P \text{ is unramified and has a non-rational extension in the case (3),} \\ N(F_6) &= 55 \quad \text{if } P \text{ is ramified in the case (3),} \\ N(F_6) &= 56 \quad \text{if } P \text{ is unramified and has 2 rational extensions in the case (3).} \end{aligned}$$

To find the genus of F_6, as usual we apply the Hurwitz Genus Formula;

$$\begin{aligned} 2 \cdot g(F_6) - 2 &= [F_6 : F_5] \cdot (2 \cdot g(F_5) - 2) + \deg Diff(F_6/F_5) \\ &\geq 2 \cdot (2 \cdot 87 - 2) + 2 \cdot 4 + 5 \cdot 6 + 5 \cdot 2 = 392, \end{aligned}$$

i.e., $g(F_6) \geq 197$.

We now summarize our results about the behaviour of the genus and the number of rational places of F_n for all $n \leq 6$ in the following theorem.

Theorem 3.11. *For the tower $\mathcal{F} = (F_0, F_1, \ldots)$, we have the following results for F_n with $0 \leq n \leq 6$;*

	$g(F_n)$	$N(F_n)$	$N(F_n)/2^n$	$g(F_n)/2^n$	$N(F_n)/g(F_n)$
F_0 :	0	3	3	0	∞
F_1 :	1	5	2.5	0.5	5
F_2 :	5	8	2	1.25	1.6
F_3 :	14	13	1.625	1.75	~ 0.929
F_4 :	36	21	1.3125	2.25	$0.58\bar{3}$
F_5 :	87	34	1.0625	2.71875	~ 0.39
F_6 :	≥ 197	$54, 55$ *or* 56	~ 0.875	≥ 3.07	≤ 0.285

Since we do not have exact quantities in the 6^{th} step of the tower $\mathcal{F}$, we cannot go further. So we may deduce some bounds for the genus and the number of rational places of F_n for large n, which will be done in the next chapter.

4

The Asymptotic Behaviour of the Tower $\mathcal{F}$

First we introduce the notions *splitting locus* and *ramification locus*, which are useful for studying the splitting rate $v(\mathcal{F}/F_0) = \lim_{i\to\infty} N(F_i)/[F_i : F_0]$ and the genus $\gamma(\mathcal{F}/F_0) = \lim_{i\to\infty} g(F_i)/[F_i : F_0]$ of a tower $\mathcal{F}$ over $\mathbb{F}_q$.

Definition 4.1. Let $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ be a tower over $\mathbb{F}_q$. Then

(*a*) The set

$$Split(\mathcal{F}/F_0) := \{P \in \mathbb{P}_{F_0} | \deg P = 1 \text{ and } P \text{ splits completely in all extensions } F_n/F_0\}$$

is called the *splitting locus* of $\mathcal{F}$ over F_0.

(*b*) The set

$$Ram(\mathcal{F}/F_0) := \{P \in \mathbb{P}_{F_0} | P \text{ is ramified in } F_n/F_0 \text{ for some } n \geq 1\}$$

is called the *ramification locus* of $\mathcal{F}$ over F_0.

Notice that the set $Split(\mathcal{F}/F_0)$ is finite and the set $Ram(\mathcal{F}/F_0)$ may be finite or infinite. Furthermore, in the case that splitting locus is non-empty, there are several methods which are helpful to find the limit of a tower, which satisfies

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)} = \frac{v(\mathcal{F}/F_0)}{\gamma(\mathcal{F}/F_0)}.$$

(For these methods, we refer to the references.)

From now on we consider our usual tower $\mathcal{F}$ which is defined by the polynomial

$$f(X, Y) = Y^2X + Y + X^2 + 1 \quad \text{over} \quad \mathbb{F}_2.$$

By Lemma 2.5 and applying repeatedly Abhyankar's Lemma in the pyramid (for the tower $\mathcal{F}$), we see that all non-rational places of F_0 are unramified in F_n for all $n > 0$. Then we have the following lemma, which is an obvious result.

Lemma 4.2. *The tower $\mathcal{F}$ is a wild tower with empty splitting locus, and the ramification locus of $\mathcal{F}$ over F_0 is*

$$Ram(\mathcal{F}/F_0) = \{(x_0 = 0),\ (x_0 = 1),\ (x_0 = \infty)\}\ .$$

As the splitting locus of the tower $\mathcal{F}$ over F_0 is an empty set, it does not help us to find the limit of this tower. Thus, we may deduce some bounds for the number of rational places and the genus of F_n for all $n \geq 0$.

Let P be a rational place of F_n with tuple $T(P) = (k_0, k_1, \ldots, k_n)$. Recall that by Proposition 3.3, we have

- $k_n = 0 \Rightarrow k_{n+1} = 1$ or ∞,
- $k_n = 1 \Rightarrow k_{n+1} = 0$ or 1,
- $k_n = \infty \Rightarrow k_{n+1} = \infty$.

We denote by $N_0(F_n)$, $N_1(F_n)$, $N_\infty(F_n)$ the number of all tuples ending with $0, 1, \infty$ for the rational places of F_n, respectively.

Lemma 4.3. *Let $\alpha := \frac{\sqrt{5}+1}{2}$. For the tower $\mathcal{F}$, we have the following assertions; For all $n \geq 0$,*

(a) $N_1(F_n) = N_0(F_{n+1})$ *and*
(b) $N_0(F_n) = \dfrac{\alpha^{2n+2} + (-1)^n}{\sqrt{5}\alpha^{n+1}}$.

Proof. First notice that from the conditions for k_i, which are given above, we conclude that $N_0(F_0) = N_1(F_0) = 1$ and for all $n \geq 1$,

(1) $N_0(F_n) = N_1(F_{n-1})$, which gives *(b)*, and

(2) $N_1(F_n) = N_0(F_{n-1}) + N_1(F_{n-1})$.

Now from these results, we can easily infer that for all $n \geq 2$,

$$\begin{aligned} N_0(F_n) = N_1(F_{n-1}) &= N_0(F_{n-2}) + N_1(F_{n-2}), \\ &= N_0(F_{n-2}) + N_0(F_{n-1}). \end{aligned}$$

That is, $N_0(F_n)$ satisfies the Fibonacci recursion. It is well-known that the solution space of the Fibonacci recursion is a two-dimensional linear vector space which is generated by the series α^n and $(1-\alpha)^n$ with $n \geq 0$ (see [9]). Therefore, for all $n \geq 0$,

$$N_0(F_n) = r\alpha^n + s(1-\alpha)^n \quad \text{for some real } r \text{ and } s. \tag{4.1}$$

Then by using the initial values, we obtain

$$N_0(F_0) = r + s = 1, \quad \text{and} \quad N_0(F_1) = r\alpha + s(1-\alpha) = 1,$$

which yield

$$r = \frac{-\alpha}{1-2\alpha} = \frac{\alpha}{\sqrt{5}} \quad \text{and} \quad s = \frac{1-\alpha}{1-2\alpha} = \frac{\alpha - 1}{\sqrt{5}}.$$

Next, by using $1 - \alpha = \frac{-1}{\alpha}$ and substituting these values in the equation (4.1), we obtain

$$\begin{aligned} N_0(F_n) &= \left(\frac{\alpha}{\sqrt{5}}\right)\alpha^n + \left(\frac{\alpha-1}{\sqrt{5}}\right)(1-\alpha)^n \\ &= \frac{\alpha^{n+1}}{\sqrt{5}} + \frac{(-1)^n}{\sqrt{5}\alpha^{n+1}} = \frac{\alpha^{2n+2} + (-1)^n}{\sqrt{5}\alpha^{n+1}}. \end{aligned}$$

□

Theorem 4.4. *For the tower $\mathcal{F} = (F_0, F_1, F_2, \ldots)$, we have the following;*

$$9 \cdot 2^{n-2} \leq g(F_n) \leq (n-1) \cdot 2^n + 1 \quad \textit{for all} \quad n \geq 4,$$

where $g(F_n)$ denotes the genus of F_n.

To prove this theorem, we need Castelnuovo's Inequality.

Theorem 4.5 (Castelnuovo's Inequality). *Let F/K be a function field with constant field K. Suppose that there are two subfields F_1/K and F_2/K of F/K satisfying*

(a) *$F = F_1F_2$ is the compositum of F_1 and F_2,*

(b) *$[F : F_i] = n_i$, and F_i/K has genus g_i (for $i = 1, 2$).*

Then the genus g of F/K is bounded by

$$g \leq n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

Proof. See [1, p.146]. □

Proof of Theorem 4.4. For simplicity, first we set $g_n := g(F_n)$. We prove by induction. Clearly, it is true for $n = 4$ (see Theorem 3.11). Assume that

$$9 \cdot 2^{n-3} \leq g_{n-1} \leq (n-2)2^{n-1} + 1.$$

Then by the Hurwitz Genus Formula and our assumtion, we obtain

$$\begin{aligned} 2 \cdot g_n - 2 &= 2 \cdot (2g_{n-1} - 2) + \deg Diff(F_n/F_{n-1}) \\ &\geq 2^2 \cdot 9 \cdot 2^{n-3} = 9 \cdot 2^{n-1}, \end{aligned}$$

which yields

$$g_n \geq 9 \cdot 2^{n-2}.$$

For the second inequality, notice that $F_n = F_{n-1}\mathbb{F}_2(x_{n-1}, x_n)$ with $[F_n : F_{n-1}] = 2$, $[F_n : \mathbb{F}_2(x_{n-1}, x_n)] = 2^{n-1}$ and $g(\mathbb{F}_2(x_{n-1}, x_n)) = g_1 = 1$ by Theorem 3.11. Then by Castelnuovo's Inequality and the induction hypothesis,

$$\begin{aligned} g_n &\leq 2 \cdot g_{n-1} + 2^{n-1} + 2^{n-1} - 1 \\ &\leq 2 \cdot \left[(n-2)2^{n-1} + 1\right] + 2^n - 1 \\ &= (n-1)2^n + 1 \end{aligned}$$

□

Next, for the number of rational places $N(F_n)$, we have the following result:

Theorem 4.6. *For the tower $\mathcal{F} = (F_0, F_1, \ldots)$, for all $n \geq 0$, we have*

$$\alpha^n \leq N(F_n) \leq 3 \cdot 2^n \quad \textit{where} \quad \alpha = \frac{\sqrt{5}+1}{2}.$$

Proof. We know that all function fields F_n (for all $n \geq 0$) have the same constant field $\mathbb{F}_2$, and so all rational places of F_n must lie over the rational places of F_0. Therefore, if all rational places of F_0 split in F_n, then since each of these places have 2^n rational extensions in F_n, we get $N(F_n) = 3 \cdot 2^n$. Otherwise, we have $N(F_n) < 3 \cdot 2^n$.

Now let P be a rational place of F_{n-1} for $n \geq 1$ with the tuple $T(P) = (k_0, \ldots, k_{n-1})$. Then from Proposition 3.3, we know that if $k_0 = 0$ or 1, then P splits in F_n. So there are at least $2 \cdot N_0(F_{n-1}) + 2 \cdot N_1(F_{n-1})$ rational places of F_n. Therefore, by using Lemma 4.3, we get

$$\begin{aligned} N(F_n) &\geq 2N_0(F_{n-1}) + 2N_1(F_{n-1}) \\ &= 2N_0(F_{n-1}) + 2N_0(F_n) \\ &= 2N_0(F_{n+1}) = 2\left(\frac{\alpha^{2n+4} + (-1)^{n+1}}{\sqrt{5}\alpha^{n+2}}\right) \geq \alpha^n. \end{aligned}$$

□

Finally, note that the bounds that we have found for the genus and the number of rational places of F_n (for $n \geq 0$) are not enough to determine the asymptotic behaviour of the tower $\mathcal{F}$. That is, we do not know whether it is an asymptotically good or bad tower. Therefore, the following problem is still open.

Problem: How to find non-constant polynomials which define asymptotically good towers over the prime fields $\mathbb{F}_p$?

Bibliography

[1] H. Stichtenoth, Algebraic Function Fields and Codes, *Springer, Berlin,* (2008).

[2] A. Garcia, H. Stichtenoth, M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997) 257-274.

[3] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61** (1996) 248-273.

[4] A. Garcia, H. Stichtenoth, Asymptotics for the genus and the number of rational places in towers of function fields over a finite field, *Finite Fields Appl.* **11** (2005) 434-450.

[5] P. Beelen, A. Garcia, H. Stichtenoth, Towards a classification of recursive towers of function fields over finite fields, *Finite Fields Appl.* **12** (2006) 56-77.

[6] S. Ling, H. Stichtenoth, S. Yang, A class of Artin-Schreier towers with finite genus, *Bulletin Braz Math Soc, New Series* **36(3)**, (2005) 393-401.

[7] A. Garcia, H. Sichtenoth, Explicit Towers of Function Fields over Finite Fields in "Topics in Geometry, Coding Theory and Cryptography", (A. Garcia and H. Stichtenoth, Eds.) *Algebra and Applications, Springer-Verlag* , **6** (2007) 1-59.

[8] A. Bassa, Towers of function fields over cubic fields, *Ph.D. Thesis, University of Essen,* 2006.

[9] R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics, *A Foundation For Computer Science, Addison-Wesley Publishing Company, Inc.*, (1998)